

Norton AntiVirus for OS/2 User's Guide

SYMANTEC.TM

NORTON

AntiVirusTM

FOR OS/2®

Norton AntiVirus for OS/2 User's Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright Notice

Copyright © 1998 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make change without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, Peter Norton Group, 10201 Torre Avenue, Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are trademarks of Symantec Corporation.

OS/2 is a registered trademark of IBM Corporation in the United States and other countries. Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

SYMANTEC LICENSE AND WARRANTY

NOTICE: SYMANTEC LICENSES THE ENCLOSED SOFTWARE TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THE LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY BEFORE OPENING THIS PACKAGE, AS OPENING THE PACKAGE WILL INDICATE YOUR ASSENT TO THEM. IF YOU DO NOT AGREE TO THESE TERMS, THEN SYMANTEC IS UNWILLING TO LICENSE THE SOFTWARE TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE FULL PRODUCT WITH PROOF OF PURCHASE TO THE DEALER FROM WHOM IT WAS ACQUIRED WITHIN SIXTY DAYS OF PURCHASE, AND YOUR MONEY WILL BE REFUNDED.

LICENSE AND WARRANTY

The software which accompanies this license (collectively the "Software") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. Except as may be modified by a license addendum which accompanies this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

- (i) use that number of copies of the appropriate titles of the software as have otherwise been licensed to you by Symantec under a Symantec Volume Incentive or Value License, provided that the number of copies of all such titles in the aggregate will not exceed the total number of copies so indicated on such Volume Incentive or Value license;
- (ii) make one copy of the Software for archival purposes, or copy the software onto the hard disk of your computer and retain the original for archival purposes;
- (iii) use the Software on a network, provided that you have a licensed copy of the Software for each computer that can access the Software over that network;
- (iv) after written notice to Symantec, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software and the transferee agrees to the terms of this agreement; and
- (v) if a single person uses the computer on which the Software is installed at least 80% of the time, then after

returning the completed product registration card which accompanies the Software, that person may also use the Software on a single home computer.

You may not:

- (i) copy the printed documentation which accompanies the Software;
- (ii) sublicense, rent or lease any portion of the Software;
- (iii) reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- (iv) use a previous version or copy of the Software after you have received a disk replacement set or an upgraded version as a replacement of the prior version, unless you donate a previous version of an upgraded version to a charity of your choice, and such charity agrees in writing that it will be the sole end user of the product, and that it will abide by the terms of this agreement. Unless you so donate a previous version of an upgraded version, upon upgrading the Software, all copies of the prior version must be destroyed;
- (v) use the server based software products included with the Software if you have not licensed the Norton AntiVirus Solution for server-based products;
- (vi) use the suite based software products included with the Software if you have not licensed the Norton AntiVirus Solution Suite;
- (vii) use other than the Macintosh versions of the software if you have only licensed the Macintosh versions of the software; or
- (viii) use a later version of the Software than is provided herewith unless you have purchased upgrade insurance or have otherwise separately acquired the right to use such later version.

Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

Disclaimer of Damages:

REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU. IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 CFR 52.227-19, as applicable, Symantec Corporation, 10201 Torre Avenue, Cupertino, CA 95014.

General:

This Agreement will be governed by the laws of the State of California. This Agreement may only be modified by a license addendum which accompanies this license or by a written document which has been signed by both you and Symantec. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write:

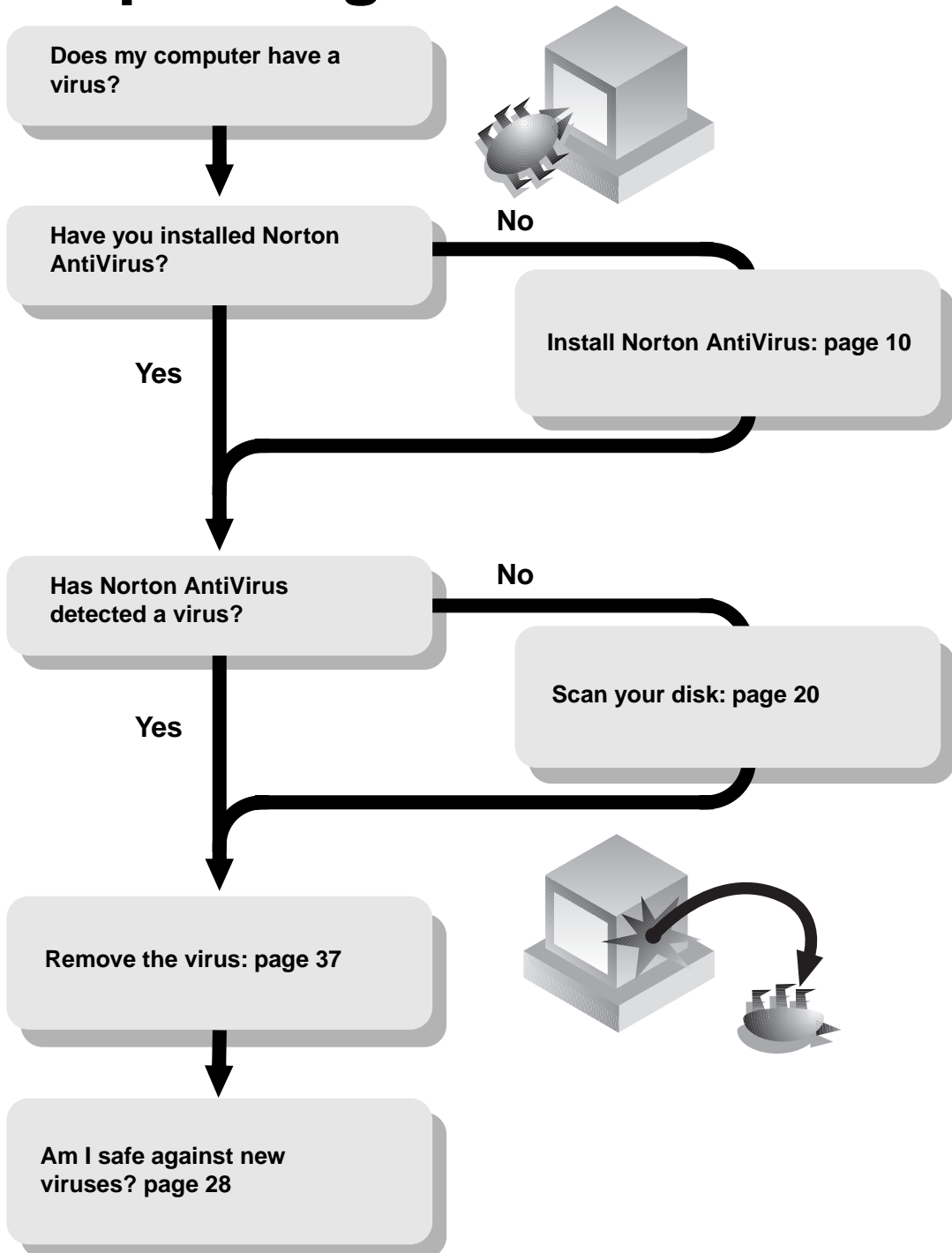
Symantec Customer Service, 175 W. Broadway, Eugene, OR 97401. Symantec, the Symantec logo, Norton AntiVirus, SAM, and SAM Administrator are U.S. registered trademarks of Symantec Corporation. Microsoft, Windows, and Windows NT are registered

trademarks of Microsoft Corporation. OS/2 is a registered trademark of IBM Corporation. Other brands and products are trademarks of their respective holder/s. © 1998 Symantec Corporation. All rights reserved. Printed in the U.S.A. Manufactured under an NSAI registered ISO 9002 quality system. 21088 2/98 07-70-00896

SYMANTEC SOFTWARE LICENSE ADDENDUM

Notwithstanding any of the terms and conditions contained in the Symantec Software License, you may make and use up to that number of copies of the Software that is indicated on the License Authorization Coupon contained in your box. The coupon will constitute proof of your right to make and use such additional copies.

Help! I've got a virus!



C O N T E N T S

Chapter 1 Installation

About Norton AntiVirus for OS/2	9
Requirements for installing	10
If you think you have a virus	10
Installing Norton AntiVirus OS/2	10
Questions when installing	12
What to do after installing	13
Uninstalling Norton AntiVirus	14

Chapter 2 Using Norton AntiVirus for OS/2

About computer viruses	15
What viruses do	15
What viruses don't do	16
About computer viruses in OS/2	16
About Win-OS/2 and DOS sessions	16
What Norton AntiVirus does	17
What you have to do	17
Tips for avoiding viruses	18
Starting Norton AntiVirus	18
Scanning for viruses	19
Scanning drives	20
Scanning network drives	20
Scanning files or folders	22
Scheduling scans and updates	23
Customizing Norton AntiVirus	26
Using Norton AntiVirus Auto-Protect	26
Temporarily disabling or enabling Auto-Protect	26
Verifying that Auto-Protect is active	27
Keeping virus protection current	28
Updating virus protection with LiveUpdate	28
Viewing Norton AntiVirus activity	31
Filtering Activity Log events	31
Viewing the virus list	32
Using the command-line scanner	34

Chapter 3 **Eradicating Viruses**

What to do if a virus is found	37
Virus Alerts in DOS and Win-OS/2 sessions	38
Types of virus alerts	39
VIRUS FOUND	39
VIRUS-LIKE ACTIVITY	39
Quick guide to alert actions	40
What to do if Norton AntiVirus can't repair	41
Infected files	41
Compressed files	42
Hard disk master boot record or boot record	43
Floppy disk boot record	43
System file	43
Using the DOS Emergency Boot Disk Set	44
Creating OS/2 System floppy disks	45

Chapter 4 **Customizing Norton AntiVirus**

Customizing scanning options	49
Selecting which files to scan	51
Managing program file extensions	52
Setting advanced scanning options	54
Customizing virus response	55
Scanning for unknown viruses	56
Customizing Auto-Protect	57
Monitoring the files you use	57
Monitoring for unknown viruses	60
Monitoring for virus-like activities	60
Monitoring floppy disks	62
Customizing startup options	63
Customizing the activity log	64
Excluding files from scans	65
Managing the exclusions list	65
Adding an exclusion	66
Password-protecting Norton AntiVirus	69
Removing password protection	71

Symantec Service and Support Solutions

Index

Installation

About Norton AntiVirus for OS/2

Norton AntiVirus is the most comprehensive virus prevention, detection, and elimination software available for your computer. You can use Norton AntiVirus to scan an entire disk (or disks), a particular directory and all of its files, or a specific file.

Norton AntiVirus' features include:

- On-demand scanning of local or network hard disks, floppy disks, paths, folders, and individual files.
- Automated virus definition updates via Live Update, to keep your virus protection up to date.
- Configurable scheduling feature so you can schedule automatic scans at a time most convenient for you.
- Automatic protection within Win-OS/2 and DOS sessions, for complete protection for all activities within the sessions.

When you run an application in a DOS or Win-OS/2 session, the automatic protection feature, Norton Auto-Protect, loads into your computer's memory, providing constant protection while your work in that session. In a DOS or Win-OS/2 session, Microsoft Word and Excel data files are protected from cross-platform macro viruses by Auto-Protect, which scans data files when you open, copy, or save them.

Requirements for installing

Your minimum computer requirements are:

- IBM PC or 100% compatible
- Intel 80386 DX or higher (Intel 486 recommended)
- OS/2 2.11, Warp, Warp Connect, or Warp 4
- 16 MB of RAM (32 MB RAM recommended)
- 24 MB of disk space
- CD-ROM drive

If you think you have a virus

If you think you have a virus, you should use the DOS Emergency Boot Disk Set to scan your system before you install Norton AntiVirus for OS/2. The Emergency Boot Disk Set is a set of two DOS-based floppy disks that are supplied with your package. They let you restart your computer and scan for boot viruses. For more information, see [“Using the DOS Emergency Boot Disk Set”](#) on page 44.

Installing Norton AntiVirus OS/2

The following issues should be considered before installing Norton AntiVirus for OS/2 on a workstation. For specific considerations when installing OS/2 on a network server, see the “Norton AntiVirus Solution Implementation Guide.”

- Norton AntiVirus automatically detects and uninstalls IBM Anti-Virus when you install.
- You should scan for viruses & run LiveUpdate after installation. For more information, see [“What to do after installing”](#) on page 13.
- You can configure the Scheduler, Auto-Protect, and other scanning features after you have installed Norton AntiVirus.

To configure the Scheduler, see [“Scheduling scans and updates”](#) on page 23.

To configure Auto-Protect and Scanning features, see [“Customizing Norton AntiVirus”](#) on page 47.

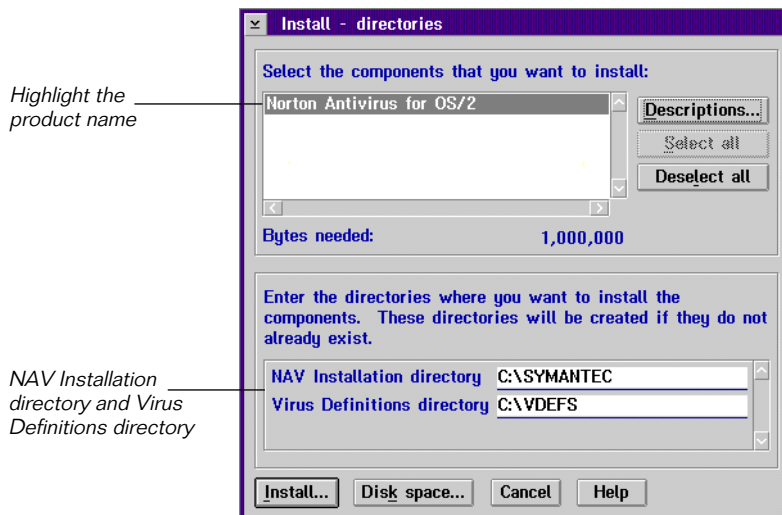
To install from a CD:

- 1 Insert the Norton AntiVirus Solutions CD in the CD-ROM drive.
- 2 From the OS/2 desktop, open the Norton AntiVirus Solutions CD window and locate the NAVOS2 folder.
- 3 Double-click the Install icon.

You can also select the Install icon, press the Mouse 2 button, and click Run.

- 4 Follow the on-screen instructions to proceed with the installation.

The Install - directories screen appears.



The NAV Installation directory and Virus Definitions directory are indicated in the Install dialog box.

- 5 Click Install to continue installing Norton AntiVirus to the directory indicated in the dialog box.

Click Disk Space to see available space on your hard disk, and how much Norton AntiVirus needs for installation. You can change hard disks if necessary.

Click Help to view more installation tips.

- 6 Follow the on-screen prompts to complete installation. If you have any questions, see [“Questions when installing”](#) on page 12.

When installation is complete, you see the following dialog box:



7 Click Finish.

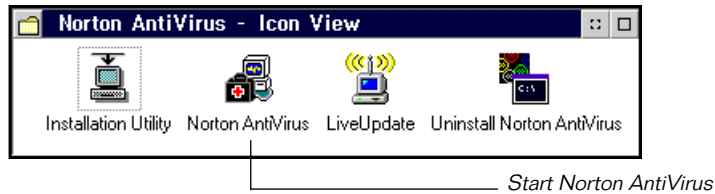
Questions when installing

Norton AntiVirus helps you install by giving you on-screen directions and highlighting the recommended actions. You are asked to make the following choices:

What the choices are	What you should do	Why?
Select the directory for Norton AntiVirus.	Accept the preset choice: C:\SYMANTEC.	There's no reason not to. The choice is there for unique circumstances, such as if you have a different boot drive letter.
Norton AntiVirus Setup needs to modify your startup files.	Click OK to let Norton AntiVirus do this for you.	If you don't have experience making changes to system files, it can be a complicated process.

What to do after installing

When you have installed Norton AntiVirus for OS/2, a Norton AntiVirus folder is created on the OS/2 Presentation Manager Desktop. From here you can start Norton AntiVirus, update or change installed components with the Installation Utility, and, if necessary, remove Norton AntiVirus with the Uninstall utility.



Once Norton AntiVirus for OS/2 is installed, do the following:

- Scan for viruses immediately after installation is complete to ensure your computer is virus-free. If the scan finds an active virus, you can remove the virus right away to prevent further possible damage. For more information, see [“Scanning for viruses”](#) on page 19.
- Schedule regular, frequent hard disk scans and LiveUpdate events. For more information, see [“Scheduling scans and updates”](#) on page 23.
- Keep Auto-Protect enabled for complete protection in Win-OS/2 and DOS sessions. For more information, see [“Using Norton AntiVirus Auto-Protect”](#) on page 26.
- Run LiveUpdate to ensure you have the most up-to-date virus protection. For more information, see [“Keeping virus protection current”](#) on page 28.
- To ensure no viruses are in memory, you can use the Emergency Boot Disk Set supplied in your package to restart your computer in DOS and scan for boot viruses. For more information, see [“Using the DOS Emergency Boot Disk Set”](#) on page 44.
- We recommend that you use your OS/2 System to create a set of OS/2 Startup Utility Diskettes in case you ever have to restart your computer from floppy disks, or restore damaged system files or boot records. For more information, see [“Creating OS/2 System floppy disks”](#) on page 45.

Uninstalling Norton AntiVirus

To uninstall Norton AntiVirus:

- 1 Double-click the Uninstall Norton AntiVirus icon in the Norton AntiVirus desktop folder.
- 2 In the dialog box that appears, highlight Norton AntiVirus.
- 3 From the Action menu, choose Delete.
- 4 In the Delete box, highlight Norton AntiVirus and click Delete.

Using Norton AntiVirus for OS/2

This chapter describes how to get the most out of Norton AntiVirus for OS/2. It explains what viruses are, how to use Norton AntiVirus to protect your computer and prevent the spread of infection, and how to update virus definitions to maintain complete protection.

About computer viruses

A computer virus is, simply, a computer program written by an ill-intentioned programmer. Your computer can catch a virus from disks, a local network or the Internet. Just as a cold virus attaches itself to a human host, a computer virus attaches itself to a program. And just like a cold, it's contagious.

What viruses do

- Take control of your computer without your knowledge.
- Cause your computer to behave strangely, for example, beep or display annoying messages.
- Hide in macros that infect and spread throughout Word and Excel documents. (These are called macro viruses.)
- Cause serious destruction to your files. Viruses can damage data, delete files, and can even completely erase your hard disk.
- Remain inactive until a predetermined trigger date (for example, Friday the 13th) to wreak havoc.

What viruses don't do

- Infect or damage hardware, such as keyboards or monitors. You may experience strange behaviors (such as characters appearing upside down) but your disks are not physically damaged, just what is stored on them.

About computer viruses in OS/2

There are very few computer viruses native to OS/2. There are, however, thousands of viruses native to Windows and DOS, with hundreds of new viruses appearing every month. The DOS viruses are especially dangerous to OS/2 system boot sector files, the essential files that run when you start your computer.

If you have an infected data file on your computer, you may not know you have a virus because it is not active in OS/2. However, if you send that file to someone working in a Windows or DOS environment, that file could infect their computer and cause damage.

About Win-OS/2 and DOS sessions

OS/2 provides the ability to run Windows and DOS in OS/2, running “virtual” Windows and DOS environments. The Windows version of this virtual environment is called a Win-OS/2 session. The DOS version is called a DOS session. You can run either session in full-screen mode or partial screen mode.

In Norton AntiVirus for OS/2, the Auto-Protect feature is only active in Win-OS/2 and DOS sessions. We strongly encourage you to keep this protection enabled if you run Win-OS/2 or DOS sessions. If you have Auto-Protect enabled, and you start a Win-OS/2 or DOS session in either full screen or window mode, Auto-Protect will protect you from viruses during all your activities in that session, whether you are sending email, using a word processor or spreadsheet, or copying files.

For a full description of all the features in Auto-Protect, see “[Customizing Auto-Protect](#)” on page 57.

What Norton AntiVirus does

With regular scans, Norton AntiVirus safeguards your computer from virus infection, no matter what the source. Norton AntiVirus detects viruses that spread from hard drives and floppy disks, those that travel across networks, and files that are opened, copied, or saved during DOS and Win-OS/2 sessions.

- Eliminates viruses and repairs files.
- During Win-OS/2 and DOS sessions, monitors your computer for any unusual symptoms that may indicate an active virus.
- During Win-OS/2 and DOS sessions, checks for viruses every time you use software programs on your computer, floppy disks, and document files that you receive or create.
- Protects you from Internet-borne viruses when you are accessing the Internet in a DOS or Win-OS/2 session. While Auto-Protect is active in a Win-OS/2 or DOS session, it scans program and document files automatically as they are downloaded and files within compressed files when they are extracted.

What you have to do

- Scan any new files copied onto your computer, and any floppy disks you use or receive. Create a “downloads” folder to isolate incoming and downloaded files, so you can scan them before you use them. For information on how to scan, see [“Scanning for viruses”](#) on page 19.
 - Schedule regular hard disk scans to make sure your OS/2 environment remains virus-free. For more information, see [“Scheduling scans and updates”](#) on page 23.
 - Regularly obtain from Symantec updated virus definition files that Norton AntiVirus needs to keep your virus protection up-to-date. You can do this easily with LiveUpdate. To update virus protection, see [“Keeping virus protection current”](#) on page 28.
- If you don't update regularly, you are not protected against viruses that have been released into the computer world since you installed Norton AntiVirus.

Tips for avoiding viruses

To avoid computer viruses, follow these rules:

- Install Norton AntiVirus exactly as directed to ensure you are fully protected.
- Be sure Norton AntiVirus Auto-Protect is enabled at all times when you are working in Win-OS/2 or DOS sessions.
- Use Scheduler to schedule regular scans.
- Regularly run LiveUpdate to obtain the latest virus protection files from Symantec. This ensures that you keep up with the new viruses that have been released since you installed Norton AntiVirus.
- Buy legal copies of all software you use and make write-protected backup copies.
- Scan all files on disks you receive from other people. To scan a file or a floppy disk, see “[Scanning for viruses](#)” on page 19.

Starting Norton AntiVirus

From the Norton AntiVirus main window you can initiate scans, schedule automatic scans, change how Norton AntiVirus works, or use LiveUpdate to get the latest virus protection files directly from Symantec.

To open the Norton AntiVirus window:

- 1 In the OS/2 Presentation Manager desktop, open the Norton AntiVirus folder.

2 Double-click the Norton AntiVirus icon.



To get help using Norton AntiVirus:

- 1 Select Contents from the Help menu.
- 2 Locate a topic in the Help window that appears.

To close Norton AntiVirus:

- On the Norton AntiVirus main window, click the Exit button.

Scanning for viruses

You can scan local drives, network drives, floppy disks, and individual files and folders. As well as conducting regular hard disk scans, we recommend you scan all floppy disks before you use them.

Your scan options may vary, depending on the settings in the Norton AntiVirus Options dialog box, accessible from the main window. For example, scanning network drives may not be available if that option has not been set in the Options dialog box.

Scanning drives

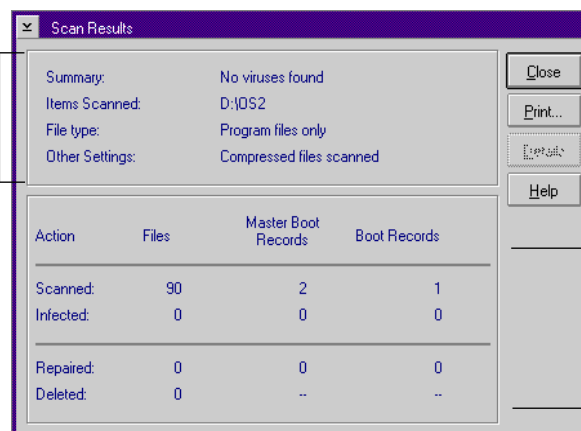
Depending on the options that have been set, you can scan local hard drives, removable drives including floppy disks, cartridge drives, and so on, paths, and network drives.

To scan drives for viruses:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, do one of the following:
 - Select specific drives in the Drives list box.
 - Select multiple drives by checking items in the Drive Types group box.
- 3 Click Scan Now.

Norton AntiVirus scans for viruses and displays a summary of the results.

Summary of scan results and options used for this scan



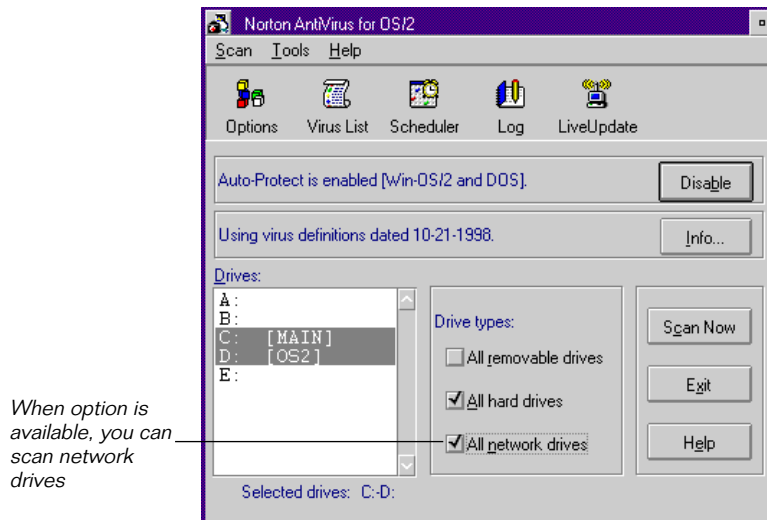
Total files and boot records scanned, infected, repaired, and deleted

If a virus or other problem is found, an alert or Problems Found dialog box appears. For more information on responding to virus alerts, see [“What to do if a virus is found”](#) on page 37.

Scanning network drives

If Allow Network Scanning is selected in the Scanner Advanced Settings dialog box ([page 54](#)) and your computer is connected to a network, you can also scan network drives. If the Allow Network Scanning option is not

selected, the All Network Drives option on the Norton AntiVirus main window is unavailable.



Because you do not always have the same access privileges to a network drive as you have on a local drive, there are some restrictions when scanning network drives with Norton AntiVirus.

Drive Access Privileges	Operations You Can Perform
None	None
Read-only	Scan
Read-Write	Scan, repair, delete

Note: Scanning network drives is more time-consuming than scanning local drives, partially because others may be creating, deleting, or moving files on a drive while Norton AntiVirus is scanning. Keep that in mind when planning to scan network drives.

For information on setting network drive options, see “[Setting advanced scanning options](#)” on page 54.

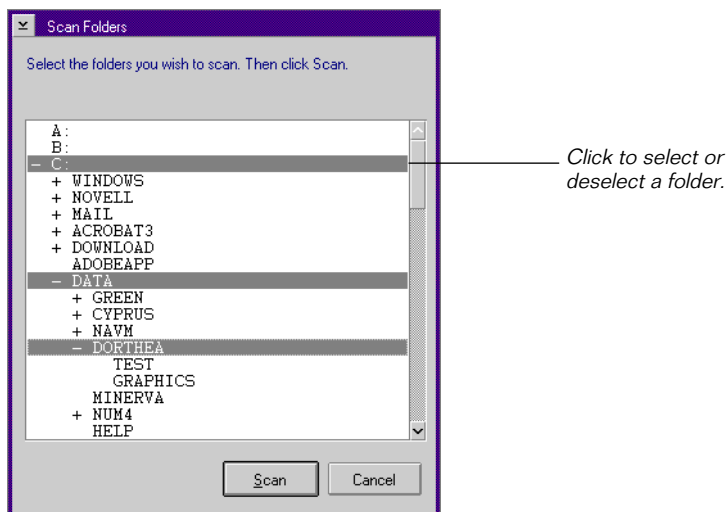
Scanning files or folders

If you just want to scan a selected area of your disk, you can select a folder, path, or file to scan. For example, if you create a “downloads” folder for incoming files, you can scan that folder before using the files.

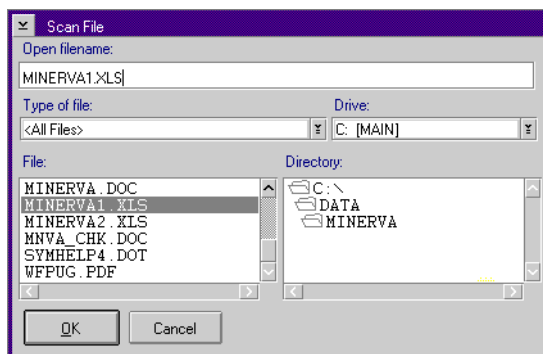
To scan individual folders, paths, or files:

- 1 Start Norton AntiVirus.
- 2 From the Scan menu at the top of the Norton AntiVirus main window, choose Folder, Path, or File.

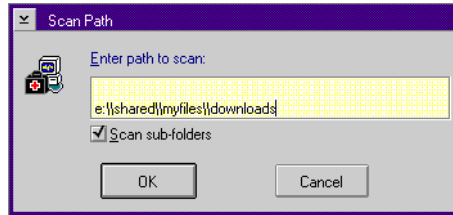
When you choose Folder, you can select a directory in the Scan Folders dialog box.



- 3 When you choose File, browse to the file, select it, and click OK.



- 4 When you choose Path, type in the path name.

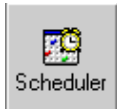


- 5 Select the Scan Sub-folders checkbox to include them in the scan.
Norton AntiVirus scans the file or folder and displays the results.

Scheduling scans and updates

You should schedule a weekly scan as soon as you have installed Norton AntiVirus. A weekly scheduled scan ensures that your computer stays virus-free. You might also want to create a “downloads” folder where you copy all incoming files, and schedule a daily scan of that folder.

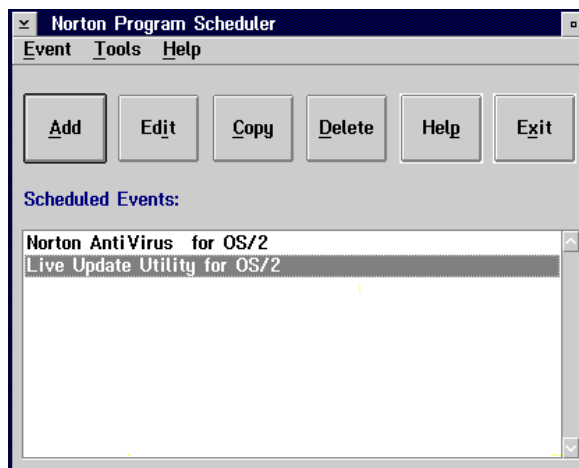
Note: You must keep the Scheduler open for scheduled events to occur. Keep it minimized on the Presentation Manager Desktop.



To schedule a scan or LiveUpdate:

- 1 In the Norton AntiVirus main window, click the Scheduler button.

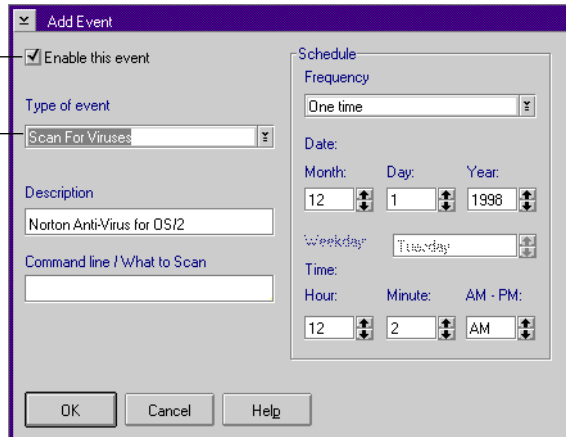
In the Scheduler window you can view currently scheduled events, and enable, add, modify, or delete a scheduled event.



- 2 Click Add.
- 3 In the Add Event dialog box, select an event from the Type of Event list:

Check to activate this event

Select an event from the list



You can select from the following events:

- Scan for Viruses
Causes the Scheduler to run Norton AntiVirus and scan the disks, folders, or files you specify in the What to Scan text box.

- Run LiveUpdate
Causes the Scheduler to run LiveUpdate on the schedule you specify.
 - Run Program
Causes the Scheduler to run the program you specify in the Command Line text box.
 - Display Message
Causes the Scheduler to display a message you type in the Message to Display text box.
- 4 In the Description text box, type a description to help you recognize the event in the Scheduler main window, for example, "Scan at 5 p.m. weekdays".
 - 5 If you choose a Scan event, enter the following:
 - In the Command Line/What to Scan text box, enter the drive letter, path, or folder to scan.
Type /L to scan all local drives.
 - For the frequency, choose Daily, Weekly or another frequency.
Daily is recommended for scans.
Weekly is recommended for LiveUpdate.
 - 6 Depending on the type of event, you can enter the day, hour, and minute you want the event to begin.
 - 7 Click Enable This Event. You must check this box or the event will not occur.
 - 8 Click OK to return to the Scheduler window.
 - 9 On the Scheduler System menu, choose Minimize.
You can also click Exit to return to the Norton AntiVirus main window.

Note: Your computer must be turned on and Norton Scheduler must be running when the scan is due to take place.

To edit, copy, or delete a scheduled event:

- 1 In the Norton AntiVirus main window, click the Scheduler button.
- 2 In the Scheduler window, select a scheduled event in the list of events.

- To change an event, click the Edit button, then follow the steps in the previous procedure to make changes to the Edit Event dialog box, or click the Help button for more assistance.
 - To copy a scheduled event, (for example, to save time when adding a new scheduled event) click Copy.
 - To delete the scheduled event, click Delete.
- 3** On the Scheduler System menu, choose Minimize.
- You can also click Exit to save changes and return to the Norton AntiVirus main window.

Customizing Norton AntiVirus

You can change the preset options to customize the way virus protection works. For complete information on customizing Norton AntiVirus, see “Customizing Norton AntiVirus” on page 47.

Using Norton AntiVirus Auto-Protect

Norton AntiVirus Auto-Protect automatically scans files that are accessed during DOS or Win-OS/2 sessions, and prompts you when a virus is found. You can temporarily disable Auto-Protect from the Norton AntiVirus main window (see “Temporarily disabling or enabling Auto-Protect” below), or change its default settings from the Options dialog box (see “Customizing Auto-Protect” on page 57).

Note: Auto-Protect does not work in OS/2 native mode. This means that during any OS/2 Presentation Manager or command-line activities, such as copying, moving, or creating files, or downloading files from the Internet, floppy disks, or network drives, you are not automatically protected against viruses.

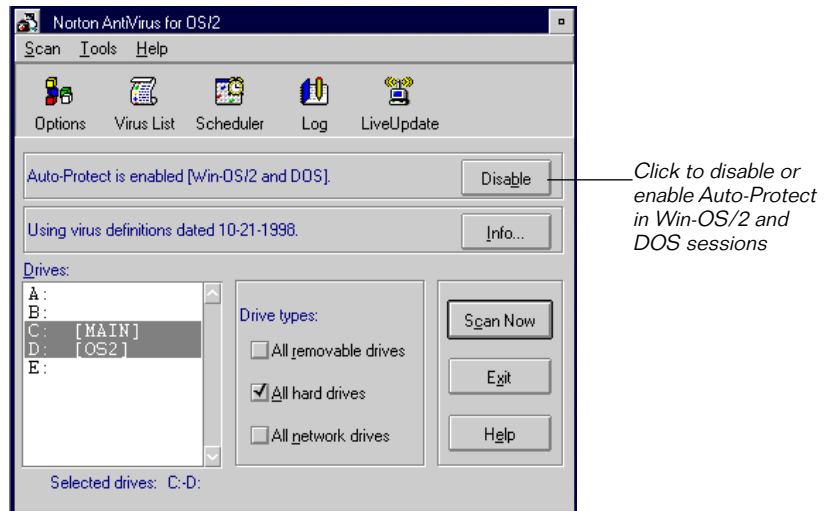
Temporarily disabling or enabling Auto-Protect

Auto-Protect is turned on when you install Norton AntiVirus for OS/2. If you run Win-OS/2 or DOS sessions, you should ensure that Auto-Protect is turned on when you start your computer. That way, whenever you start a Win-OS/2 or DOS session, you are automatically protected. For more information on changing Auto-Protect settings, see “Customizing Auto-Protect” on page 57.

The Enable/Disable button on the Norton AntiVirus main window lets you turn Auto-Protect on or off temporarily.

To turn Norton AntiVirus Auto-Protect on or off temporarily:

- 1 Start Norton AntiVirus.



- 2 In the Norton AntiVirus main window, click the Enable/Disable button.

Auto-Protect is now temporarily enabled or disabled in DOS and Win-OS/2 sessions.

- 3 Click Exit.

Note: If you have existing Win-OS/2 or DOS sessions open, there will be a brief lag before Auto-Protect will protect them.

Verifying that Auto-Protect is active

You can check to see if Norton AntiVirus Auto-Protect is active and protecting your Win-OS/2 or DOS sessions.

If the Norton AntiVirus main window shows the Disable button, it indicates that Auto-Protect is active.

You can also check Auto-Protect status in the following ways:

- Look for an Auto-Protect message on the command line when you open a DOS session window, similar to the following message:
`NAV TSR is resident.`

To change the way Auto-Protect protects your DOS and Win-OS/2 setting, use the Options settings described in “Customizing Auto-Protect” on page 57.

Keeping virus protection current

Norton AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons you get viruses is that you have not updated your virus definitions since you bought the product. Symantec provides regular, online access to these virus definitions files.

New viruses are being written all the time. You have to regularly obtain files from Symantec that contain the latest virus protection. OS/2 virus definition files are updated on a monthly basis.

Updating virus protection with LiveUpdate



Use LiveUpdate to ensure that you have the most current virus protection. LiveUpdate automatically downloads and installs virus definition files from Symantec's FTP site or from a local or network drive.

LiveUpdate is the easiest way to keep virus protection current because it downloads and installs the virus definition files automatically. You can get virus protection updates any time by clicking the LiveUpdate button. You can also configure the Scheduler to run LiveUpdate regularly.

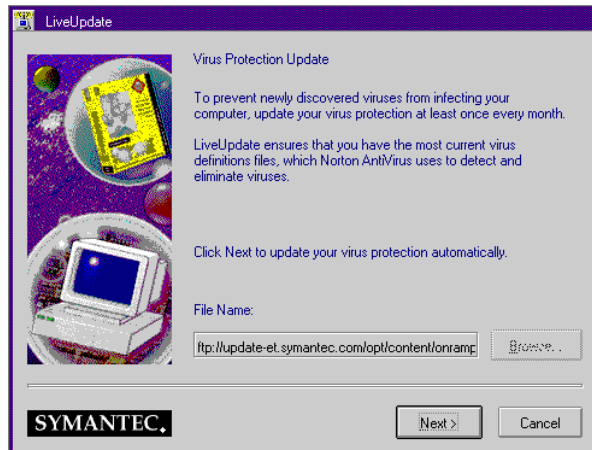
If you update virus definitions over the Internet, you will connect to Symantec's FTP server to download and install the latest virus definition files. The correct FTP path and filename should appear in the File Name text box automatically.

If you update virus definitions from an internal network, LiveUpdate lets you browse to the path and location of the virus definitions compressed file.

To run LiveUpdate with an existing Internet connection:

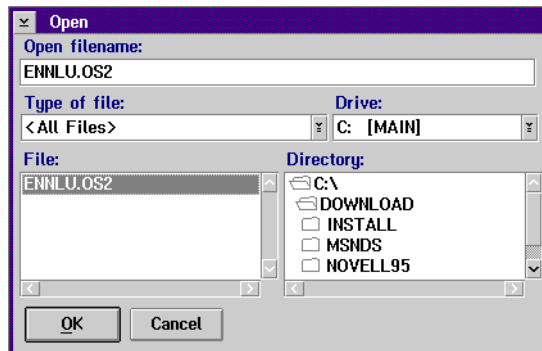
- 1 Start Norton AntiVirus.
- 2 Click the LiveUpdate button in the Norton AntiVirus main window.

By default, LiveUpdate goes to Symantec's FTP site to download the latest virus definitions file.



- 3 Click Next.

If your virus update path is on an internal network, click the Browse button and locate the virus definitions update file.



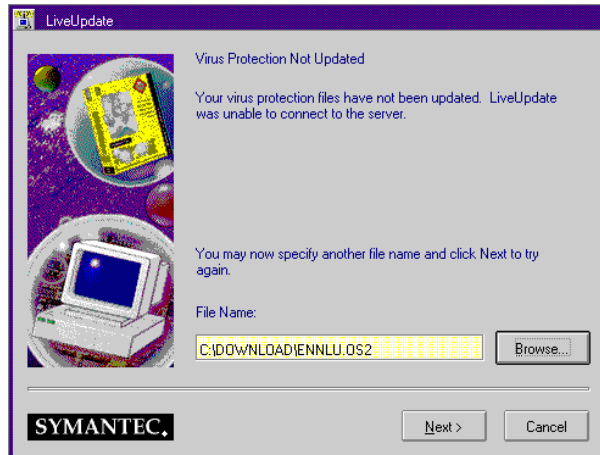
Ensure that the path and virus definitions packet filename (ENNLU.OS2) displayed in the File Name window are correct.

- 4 Click OK.

The new path appears in the LiveUpdate File Name text box.

- 5 Click Next.

LiveUpdate proceeds to connect to the designated FTP site or designated drive and path, download the latest virus definitions, and install them on your workstation.



When the update is complete, LiveUpdate displays a message.



- 6 Click Finish.

LiveUpdate has now completed the update of your virus definition files. You can view the date of your virus definitions on the Norton AntiVirus main window.

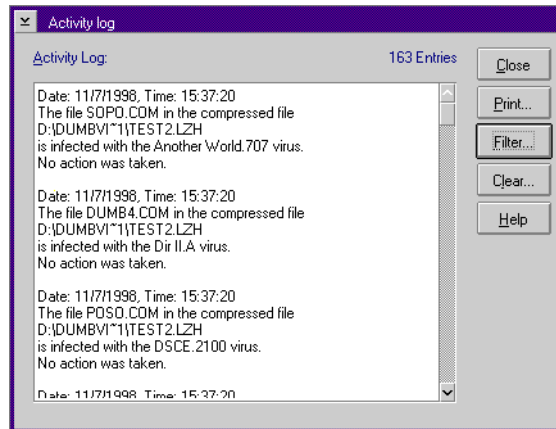
Viewing Norton AntiVirus activity



The Activity Log lets you keep track of scans, viruses, and other activities that you can specify.

To view the activity log:

- 1 In the Norton AntiVirus main window, click Log.



The Activity Log lists scanning activities. In addition, you can specify other items to be included in the log.

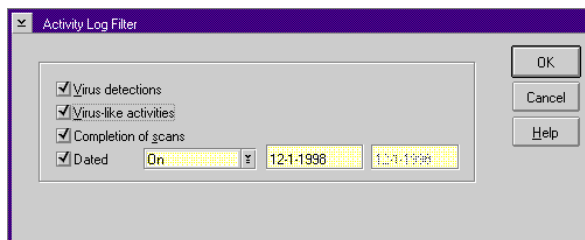
- 2 You can do the following in the Activity Log:
 - Use the scroll bar to scroll up and down to view events.
 - Apply a filter to hide selected items from view. See [“Filtering Activity Log events”](#) below.
 - Click Clear to delete all entries in the log.
 - Click Print to print the contents of the log.
- 3 Click Close to return to the Norton AntiVirus main window.

Filtering Activity Log events

You can hide Activity Log items so you can view other items more easily, without having to scroll through many events. The Activity Log Filter dialog box lets you select types—or classes—of events to display in the Activity Log list. For example, you may wish to filter out the log of daily scheduled scans so you can more easily view any virus detections that have occurred.

To filter Activity Log events:

- 1 In the Activity Log window, click Filter.



- 2 In the Activity Log Filter dialog box, select the following options:
 - Virus detections
Displays all virus detections in the log.
 - Virus-like activities
Displays all virus-like activities in the log.
 - Completion of scans
Displays all completed scans, or, when you check the Dated box, the completed scans within the date range you specify.
- 3 To display a class of items, select the checkbox.
- 4 To omit a class of items, clear the checkbox.
- 5 Click OK.

For information on configuring the Activity Log settings, including the filename, size, and type of events logged, see “[Customizing the activity log](#)” on page 64.

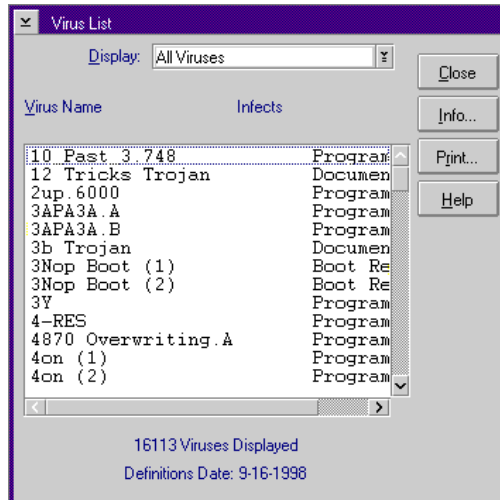
Viewing the virus list

The Virus List displays a list of viruses that Norton AntiVirus can detect and, in most cases, eliminate.

Note: It is important to update your virus definitions regularly because new viruses are discovered all the time. If you have a modem or an Internet connection, simply click LiveUpdate in the Norton AntiVirus main window. If you do not have a modem, see the User's Guide for directions on how to obtain new virus definitions from Symantec and how to update virus definitions.

To find a virus on the list:

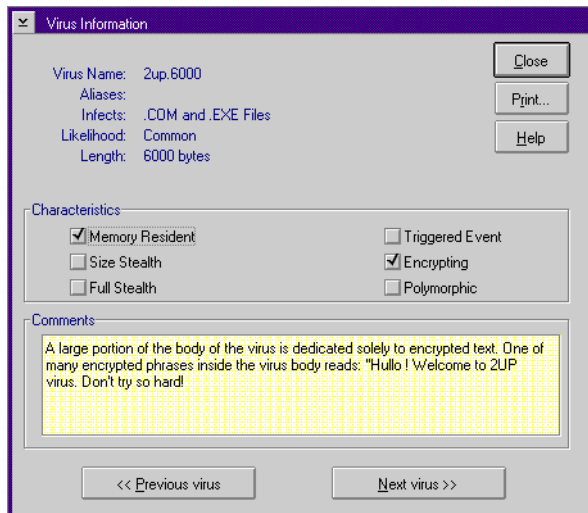
- 1 On the Norton AntiVirus main menu, click Virus List.



- 2 Use the scroll bar or type the first letter of the virus name to initiate the smart search feature to find the virus you're looking for.
- 3 Scroll until the virus you're searching for appears.

Note: To reduce the number of viruses you have to search through, choose a type of virus from the Display drop-down list box. For example, you may want to filter the Virus List to display only boot viruses or macro viruses.

- 4 Select a virus name and click Info.



Click the Help button for more information on virus categories and descriptions.

If a virus is not found on the list, the virus name may be different from what you expected. For example, the virus commonly known as Michelangelo is actually called Stoned. Michelangelo.D.

Using the command-line scanner

Norton AntiVirus for OS/2 includes a command-line scanner for OS/2 command prompt windows, named NAVDXOS2.EXE. It is used for startup scans when you start your computer. You can run this program directly from the command prompt, or by configuring a scheduled event.

You can get a list of the command-line scanner capabilities by typing the following at the OS/2 command prompt:

```
C:\SYMANTEC\NAVDXOS2 /?
```

This will print a list of command-line switches you can use with the program.

Command-line switch	Description
/?	Display the help screen.
/A	Scan all drives (A: and B: are skipped)
/L	Scan local drives (A: and B: are skipped)
/B [+ -]	Enable or disable scanning of boot records.
/BOOT	`Scan only the boot sectors of specified drives.
/S [+ -]	Enable or disable scanning subdirectories.
/REPAIR	Repair infected files automatically.
/DELETE	Delete infected files automatically.
/HALT	Halt the scanning operation if a virus is found.
/CFG:[directory]	Specify the directory containing NAVDXOS2
/LOG:file	Create and log to the specified file.
/APPENDLOG:file	Append to an existing log file.
/DOALLFILES	Scan all files, not just executables.
/NOBEEP	Run silently (no beeps).
/HELPERROR	List possible errorlevels returned by NAVDXOS2. If desired, you can run NAVDXOS2 from a batch file and process the errorlevel with IF ERRORLEVEL constructions.

Eradicating Viruses

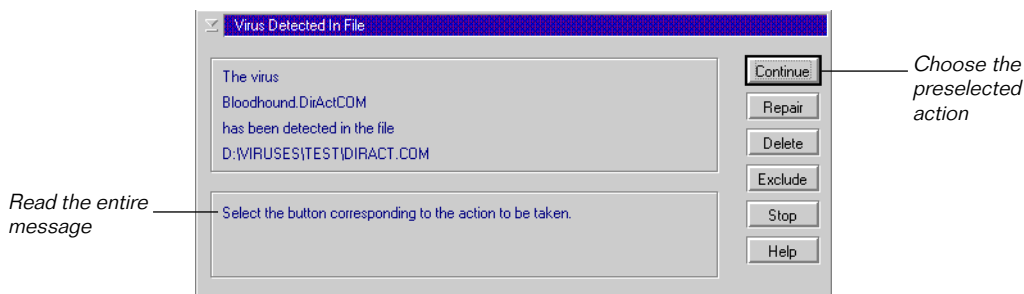
What to do if a virus is found

There are several different virus messages you might encounter when running Norton AntiVirus for OS/2. Some are generated by Auto-Protect in a Win-OS/2 or DOS session. You will need to respond to virus alerts immediately. For other alert messages, such as the Problems Found dialog box that appears after a scan, you may continue without doing anything else.

If you see a virus alert message, read it very carefully to make sure you understand the information and your options.

If you see a virus alert

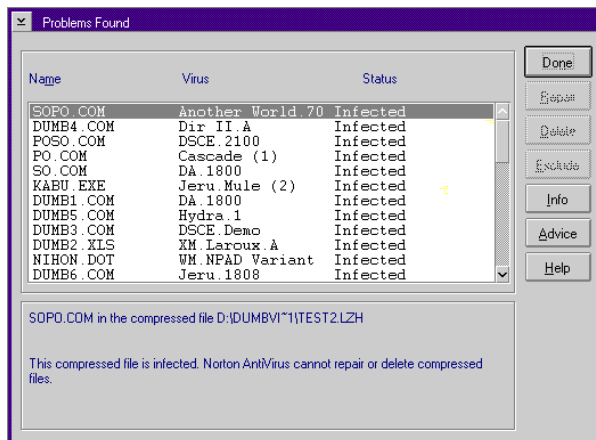
If you see a virus alert such as this example, follow the steps below.



- 1 Look for words that identify the type of problem. Read the whole message.
- 2 Choose the action that is preselected for you or follow the recommendation on the screen.
- 3 If you need more information to decide what to do, find the type of problem in the next few pages.

For example, if the message says “Virus detected in File,” look for “VIRUS FOUND.”

If you see the Problems Found dialog



- 1 Highlight an entry in the list box.
- 2 Read the message at the bottom of the dialog box.
- 3 Click Repair when infected files are found.

See “[Quick guide to alert actions](#),” on page 40 for information about the other actions.

Virus Alerts in DOS and Win-OS/2 sessions

If you are running a full screen Win-OS/2 or DOS session and Auto-Protect finds a virus, you will hear a sound. The warning message will not be visible until you switch back to the OS/2 Presentation Manager desktop. To prevent the virus from causing further damage, Norton AntiVirus will temporarily freeze the screen of your Win-OS/2 or DOS session.

If this occurs, switch immediately to OS/2 to view the alert and take action.

- To switch to OS/2, press Alt-Esc.

Types of virus alerts

VIRUS FOUND

When Auto-Protect finds a virus has infected a file on your computer, it produces a warning something like this:

VIRUS DETECTED IN FILE: The BADVIRUS virus was found in
C:\MYFILE.

To get rid of a virus infection:

- Click Repair (or type Alt-R if you can't use your mouse).

Your file is restored to exactly the way it was before the virus infected it.

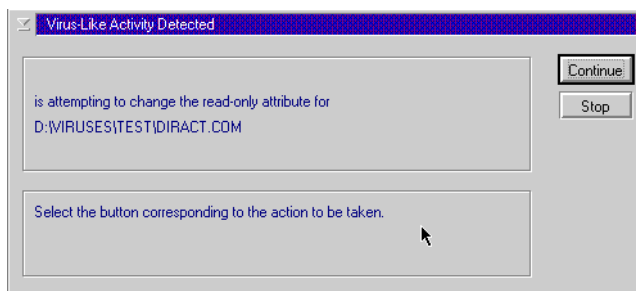
That's all you need to do. If the repair was successful, the virus is gone and your computer is safe.

Norton AntiVirus can't repair? See [“What to do if Norton AntiVirus can't repair”](#) on page 41.

VIRUS-LIKE ACTIVITY

A virus-like activity alert does not necessarily mean that your computer has a virus. It's simply a warning. It's up to you to decide whether the operation is valid in the context in which it occurred.

The alert looks something like this:



To resolve a virus-like activity alert:

Do one of the following:

- Click Continue if the message describes a valid activity for the application you are running (or type Alt+C if you can't use your mouse).



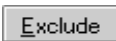


For example, if you're updating an application and the alert warns you of an attempt to write to a file, the activity is valid.

- Click Stop if the detected activity isn't related to what you are trying to do (or type S if you can't use your mouse).

For example, if you are playing a game and the alert warns you of an attempt to write to the boot records of your hard disk, the activity is invalid.

Quick guide to alert actions

If a Norton AntiVirus Auto-Protect alert appears on your screen, use this table to decide what to do. If you need more information, see the next section, "Types of virus alerts," for step-by-step instructions.

Action Buttons	When and why you use them
	For a VIRUS FOUND, Repair is always the best choice. Repair eliminates the virus and repairs the infected item automatically.
	Erases both the virus and the infected file. The virus and file are gone forever. Choose Delete if Repair is not successful. Replace a deleted file from the original program disks or backup copy. If the virus is detected again, your backup copy or original disk is infected.
	If you choose Exclude and a virus is at work, the virus won't be caught. Exclude should be used only by system administrators for system tuning.
	Continue lets you continue the current activity and ignore the virus warning.
	Halt causes the current process to stop.

What to do if Norton AntiVirus can't repair

One of the most common reasons Norton AntiVirus can't repair a file is that you don't have the most up-to-date virus protection files. Click LiveUpdate in the Norton AntiVirus main window to obtain the latest files.

Do one of the following:

- Update your virus protection and scan again. See “[Updating virus protection with LiveUpdate](#)” on page 28 for details.
- Read the information on your screen carefully to identify the type of item that can't be repaired, then match it to one of the types below:
 - Infected files are those with file names that include .COM or .EXE. Document files such as .DOC, .DOT, and .XLS can also be infected.
 - Compressed files may contain many files. You can often tell a compressed file by its name. Many compressed files end in .ZIP
 - Hard disk master boot record, boot record, or system files (such as OS2BOOT, OS2KRNL) and floppy disk boot record and system files may need to be replaced. For more information on creating OS/2 Start-Up or Utility disks, see “[Creating OS/2 System floppy disks](#)” on page 45.

Infected files

Infected files are those with file names that include .com or .exe. Document files such as .doc, .dot, and .xls can also be infected.

To respond to an infected file alert:

- Click Repair. This is usually your best option unless the alert message recommends a different action.

If Norton AntiVirus can't repair a file:

- 1 Choose Delete.
- 2 Replace the deleted document file with a backup copy or reinstall a deleted program from the original program disks.

Make sure to scan the backup disks before you use them.

If infected files can't be repaired, you need to delete them from your computer. If you leave an infected file on your computer, the virus

infection can still spread. Once deleted, the virus and the file are gone forever.

If the virus is detected again after you replace or reinstall the file, your backup copy or original program disks are probably infected. You can try contacting the manufacturer for a replacement.

Compressed files

A compressed file may contain many individual files. Norton AntiVirus can detect viruses in the individual files. However it cannot Repair, Delete, or Exclude these files until you uncompress (open up) the compressed file.

To uncompress and repair a file with PKUNZIP:

- 1 Start Norton AntiVirus.
- 2 Turn off Auto-Protect by clicking the Disable button.
- 3 From the OS/2 Presentation Manager Desktop, open a OS/2 command prompt window.
- 4 Create a temporary directory (for example, C:\TEMP).
- 5 Use PKUNZIP to uncompress the file in the temporary directory.
- 6 At the OS/2 prompt, type `NAVDXOS2 C:\TEMP*. * /REPAIR` and press Enter to scan and repair the files in the temporary directory.
- 7 If the file can't be repaired, delete it.
- 8 Recompress the files, if desired..

To uncompress with Winzip and repair in a Win-OS/2 session:

- 1 Start Norton AntiVirus.
- 2 In the Norton AntiVirus main window, turn off Auto-Protect by clicking the Disable button.
- 3 From the OS/2 Presentation Manager Desktop, open a Win-OS/2 session.
- 4 From the File Manager, create a temporary directory (for example, C:\TEMP).
- 5 Use WINZIP to uncompress the file in the temporary directory.
- 6 In the Norton AntiVirus for OS/2 main window, select Directories from the Scan menu.
- 7 Choose the C:\TEMP directory, then click Scan to scan the files again.

- 8 Let Norton AntiVirus automatically repair all the infected files.
- 9 If the file can't be repaired, delete it.
- 10 Recompress the files, if desired.
- 11 In the Norton AntiVirus for OS/2 main window, select Enable to turn Auto-Protect on again.

Hard disk master boot record or boot record

Hard disk master boot record, boot record, or system files (such as OS2BOOT or OS2KRNL) and floppy disk boot record and system files are replaced using the emergency disks or, sometimes, your OS/2 system disks.

If Norton AntiVirus can't repair your hard disk or master boot record, you may have to delete infected files and restore or reinstall your system files. We recommend that you create a set of Utility Disks so you can restart your computer and restore any damaged system files. See [“Creating OS/2 System floppy disks”](#) on page 45 for details.

Floppy disk boot record

If Norton AntiVirus cannot repair a floppy disk boot record, the virus is removed and the information on the disk is still accessible. You can safely copy all the files onto another disk. However, the floppy disk is no longer bootable.

System file

If Norton AntiVirus cannot repair a system file (for example, OS2BOOT or OS2KRNL), you have to restore the file using the OS/2 System command. See your OS/2 manual for command instructions.

Using the DOS Emergency Boot Disk Set

Sometimes a virus infection prevents your computer from starting normally. In these cases, viruses can only be removed if the computer is started from a clean disk, not the infected hard disk. In most cases, this DOS Emergency Boot Disk Set can remove active boot viruses that prevent the workstation's operating system from booting and running normally.

The DOS Emergency Boot Disk Set supplied with Norton AntiVirus lets you restart your system in DOS and automatically scan for boot viruses. It is for use when an emergency situation exists, such as when hard disk boot records or system files are infected by a virus. The DOS Emergency Boot Disk Set works on hard disks formatted in the DOS FAT file system.

In cases where your configuration requires different disk drivers, you will need to create a set of utility diskettes to reboot your system. After you have rebooted, you can then use the Norton AntiVirus Emergency Disk Set to scan your hard disk.

To use the DOS Emergency Boot Disk Set:

- 1 Shut down your computer.
- 2 Insert the DOS Emergency Boot disk in floppy drive A:.
- 3 Turn on your computer.

Your computer should restart and ask if you want to scan for viruses.

- 4 If prompted, insert the Virus Definitions disk in drive A: and press Enter.

Norton AntiVirus scans for boot and system viruses.

- 5 If a virus is found, you are prompted to repair or delete it.

When the scan is finished, Norton AntiVirus displays a status report.

- 6 Remove the floppy disk and restart your computer.

Note: After you use the DOS Emergency Boot Disk Set to remove an active virus, you must reinstall Norton AntiVirus and scan the system thoroughly to find and remove any other virus files on your hard disk. This is to ensure that no Norton AntiVirus program files were infected by the virus.

If you have any problem restarting, you may have to use your OS/2 Utility disks to restart and scan for any file damage.

Creating OS/2 System floppy disks



If your system files are damaged by a virus, you may have to restore your hard disk after you have run Norton AntiVirus and deleted the infected files.

Your OS/2 System has a utility program that creates a set of floppy disks from which you can restart your system if your hard disk becomes incapacitated. You can use these diskettes to restore essential system files to your hard disk.

Refer to your OS/2 System documentation for details on creating and maintaining a set of Utility Diskettes.

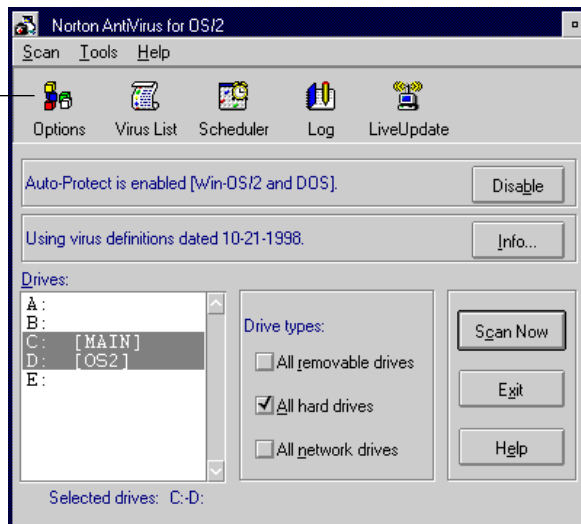
Customizing Norton AntiVirus

By default, Norton AntiVirus is installed with the most complete protection for your computer. However, you can change the settings of any option to suit your situation.

To change how Norton AntiVirus works:

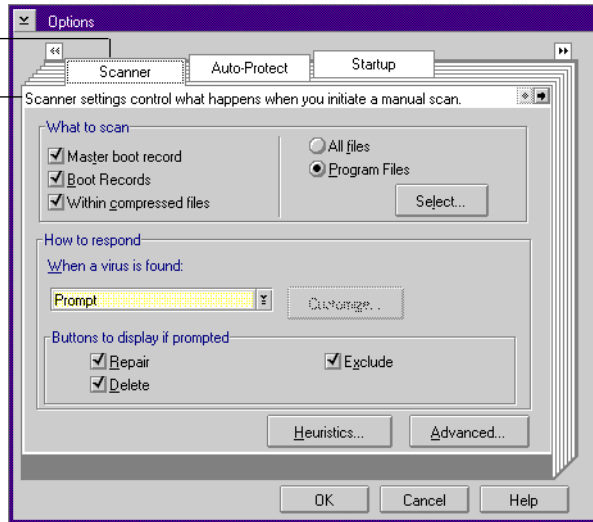
- 1 Click the Options button in the Norton AntiVirus main window.

*Click to open
the Options
dialog box*



In the Options dialog box, each tab displays a different option category.

The Options categories are divided by tabs
Description of selected tab



- 2 Click one of the tabs to bring it to the front. The top of each tab has a brief description.
- 3 Use the instructions in this chapter to change the options on all the tabs.
- 4 Click OK to close and exit the Options dialog box. (If you don't click OK, your changes are not saved.)

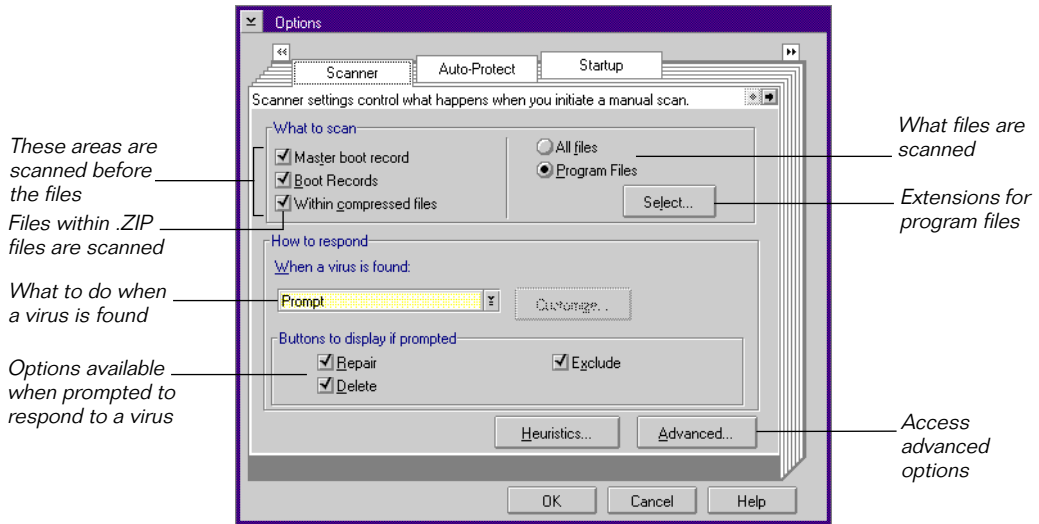
The changes you make to these settings take effect when you restart your computer.

Customizing scanning options

The settings for the Scanner category of options define what Norton AntiVirus does when you scan a file, directory, or drive using the commands in the Scan menu or using the Scan Now command button.

To modify the scanning options:

- 1 In the Options dialog box, click the Scanner tab.



- 2 Specify in the What To Scan group box the areas Norton AntiVirus scans before it scans files:
 - Master Boot Record
Checks for boot viruses in the master boot record on your hard disk.
 - Boot Records
Checks for boot viruses in the boot records on your hard disk and on any floppy disks that you scan.
 - Within Compressed Files
Have Norton AntiVirus scan files compressed using the PKZIP or WinZip utility, and ARJ (*.ARJ) and LHA (*.LZH) compressed files.

Scanning time may increase slightly if you have many .ZIP files. If you have no .ZIP files, scanning time is not affected by having this option selected.

Compressed files within compressed files are not scanned.

3 Specify what files you want to scan:

- All Files

Scans all files in the specified directory or drive (this includes files less likely to contain viruses).

- Program Files

Scans files that are most likely to become infected. Only the files with an extension that is specified in the program file extensions list are scanned.

For more information on which option to choose and on the program file extensions list, see [“Selecting which files to scan”](#) on page 51.

4 Select an option in the When A Virus Is Found drop-down list box:

- Prompt

Informs you when a virus is found and lets you choose how to respond. Click Prompt to have the most control over what happens to an infected file.

- Notify Only

Merely informs you when a virus is detected. You will not be able to repair or delete the infected file.

- Repair Automatically

Repairs an infected file or boot record without notifying you. The results of the repair are displayed at the end of the scan.

Norton AntiVirus is preset to make backup copies of files before they are repaired.

- Delete Automatically

Deletes an infected file without notifying you. Deleted files are listed at the end of the scan.

Use caution when selecting this option. Files deleted by Norton AntiVirus cannot be recovered.

- Custom Virus Response

Lets you access more options. For more information, see [“Customizing virus response”](#) on page 55.

- 5 If you selected Prompt in step 4, specify in the Buttons To Display If Prompted group box which options you want Norton AntiVirus to make available when a virus is found:
- **Repair**
Lets you repair the file or boot record. If the virus infects an item that cannot be repaired, such as a compressed file, the button is dimmed.
 - **Delete**
Lets you delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is dimmed.
 - **Exclude**
Lets you exclude the file from future checks for known viruses. Use caution when enabling this button; it can reduce your protection against viruses.

Selecting which files to scan

You can configure Norton AntiVirus to scan all files or only program files. Scanning program files only is usually sufficient, because these are the types of files from which viruses generally spread. Scanning all files takes longer, but covers any executable files that have non-standard file extensions. As a safety precaution, scan all files after a virus attack.

- **All Files**
Every file—data files (such as databases, documents, text files, and spreadsheets) and program files (such as system files, word processing programs, and utility programs)—is scanned.
- **Program Files**
Only files with extensions contained in the program file extensions list are scanned. The program file extensions list contains the most common extensions for executable files, which are most likely to become infected and spread viruses.

See “Customizing scanning options” on page 49 and “Monitoring the files you use” on page 57 for information on setting these options.

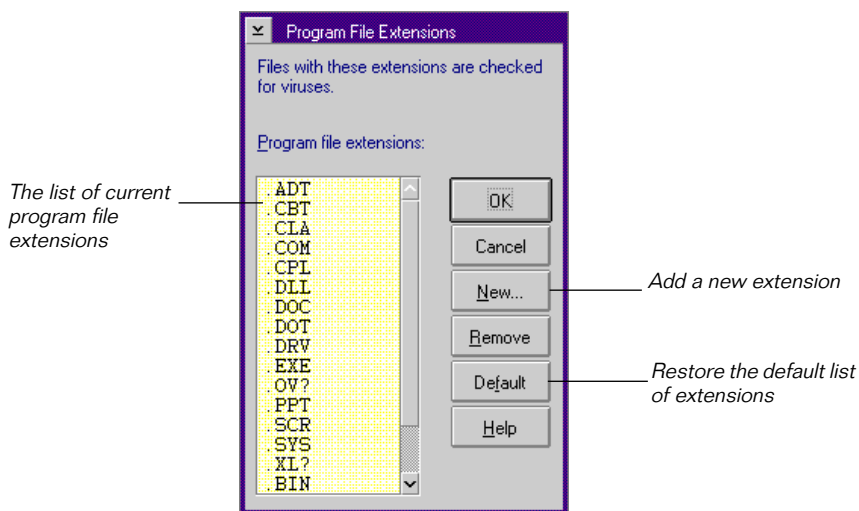
Managing program file extensions

Norton AntiVirus uses the Program File Extensions list when scanning program files. The list contains the most common extensions for executable files, which are the files most likely to become infected and spread viruses. You can view, add, edit, and delete the file extensions in this list.

Note: The extensions for Microsoft Word documents and Excel spreadsheets are included in the program files group. Although these are not program files, they can be infected by macro viruses.

To view the current program file extensions:

- 1 In the Scanner Options dialog box, select Program Files.
- 2 Click Select.



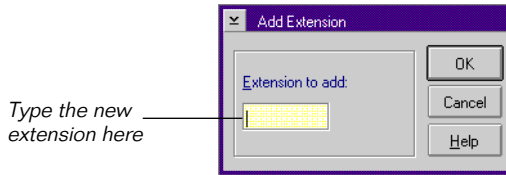
- 3 In the Program File Extensions dialog box, scroll down the list to view all the extensions.

If all your executable files' extensions are not on the list, you should add them to ensure that all appropriate files are scanned. Do not add extensions for non-executable files; viruses cannot spread from them.

Note: You can also access the Program File Extensions list from the Auto-Protect Options tab.

To add a program file extension:

- 1 Click Add in the Program File Extensions dialog box.



- 2 In the Add Extension dialog box, type the new file extension in the Extension To Add text box.

You may use wildcards in the extension, but not to represent all three characters. For example, .OV? represents files with extensions that begin with .OV, such as .OVL and .OV1.

- 3 Click OK in the Add Program File Extension dialog box.

If you find an extension in the list that you do not want Norton AntiVirus to look for, you can delete it. Be careful, files whose extensions are not on the list will not be scanned unless All Files are selected for the scan.

To delete a program file extension:

- 1 Select the file extension in the Program File Extensions list box.
- 2 Click Remove.
- 3 Click OK.

At any time, you can reset the list back to the way it looked when you installed Norton AntiVirus.

To reset the list of program file extensions:

- 1 Click Default in the Program File Extensions dialog box.

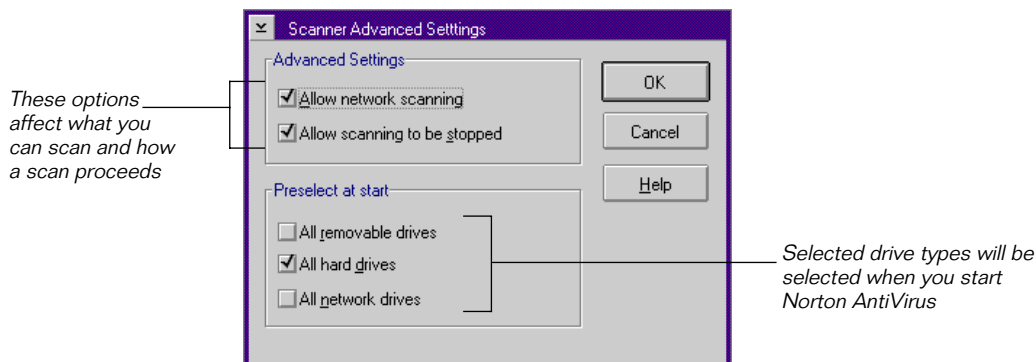
The list of extensions returns to the way it was when you installed Norton AntiVirus.

- 2 Click OK.

Setting advanced scanning options

To set additional scanning options:

- 1 Click the Advanced button in the Scanner Options dialog box.



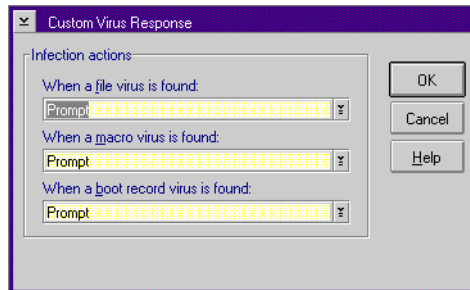
- 2 In the Scanner Advanced Settings dialog box check the options that you want to enable:
 - Allow Network Scanning
Lets you scan network drives. For more information, see [“Scanning network drives”](#) on page 20.
 - Allow Scanning To Be Stopped
Lets you halt a scan in progress. When this option is checked, the Stop button is available during a scan.
- 3 Specify in the Preselect At Start group box the drives that you want selected automatically in the Drives list box when you start Norton AntiVirus. Options are:
 - All removable drives
 - All hard drives
 - All network drives (if allow Network Scanning is checked)
- 4 Click OK.
- 5 Click OK in the Scanner Options dialog box.

Customizing virus response

If you selected the Custom Virus Response option in the When Virus Is Found list box, you can set more options.

To customize virus response:

- 1 Click the Customize button to open the Custom Virus Response dialog box.



- 2 Under When A File Virus Is Found, choose an action:
 - Prompt
Informs you when a virus is found and lets you choose how to respond. Click Prompt to have the most control over what happens to an infected file.
 - Notify Only
Informs you when a virus is detected. You will not be able to repair or delete the infected file.
 - Repair Automatically
Norton AntiVirus repairs the file. The results are recorded in the Activity Log.
 - Delete Automatically
Norton AntiVirus deletes the file automatically.
- 3 Under When A Macro Virus Is Found, choose an action:
 - Prompt (see Step 2)
 - Notify Only (see Step 2)
 - Repair Automatically (see Step 2)
 - Delete Automatically (see Step 2)

- 4 Under When A Boot Record Virus Is Found, choose an action:
 - Prompt (see Step 2)
 - Notify (see Step 2)
 - Repair Automatically (see Step 2)
- 5 Click OK to return to the Scan Options tab.

Scanning for unknown viruses

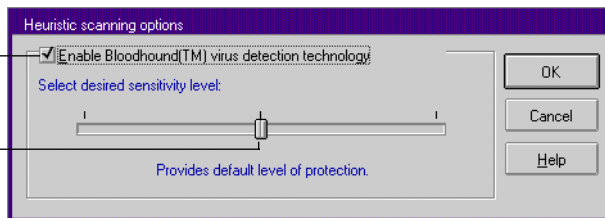
An unknown virus is one for which Norton AntiVirus does not have a definition. The Norton AntiVirus Bloodhound™ Virus Detection Technology checks the files you scan for unknown viruses. You can adjust the sensitivity level using the Heuristics button on the Scanner Options dialog box.

To scan for unknown viruses:

- 1 Click the Scanner tab.
- 2 Click Heuristics.

Do you want Norton AntiVirus to check for unknown viruses?

Select the level of vigilance



- 3 In the Heuristic Scanning Options dialog box, check Enable Bloodhound™ Virus Detection Technology to include unknown virus detection as part of your scans.
- 4 Drag the slider left or right to decrease or increase the sensitivity to virus-like activity.
- 5 Click OK.

Customizing Auto-Protect

When enabled, Norton AntiVirus Auto-Protect monitors your system for any virus activity whenever you have a DOS or Win-OS/2 session open. It alerts you when it detects an infected file or suspects a virus.

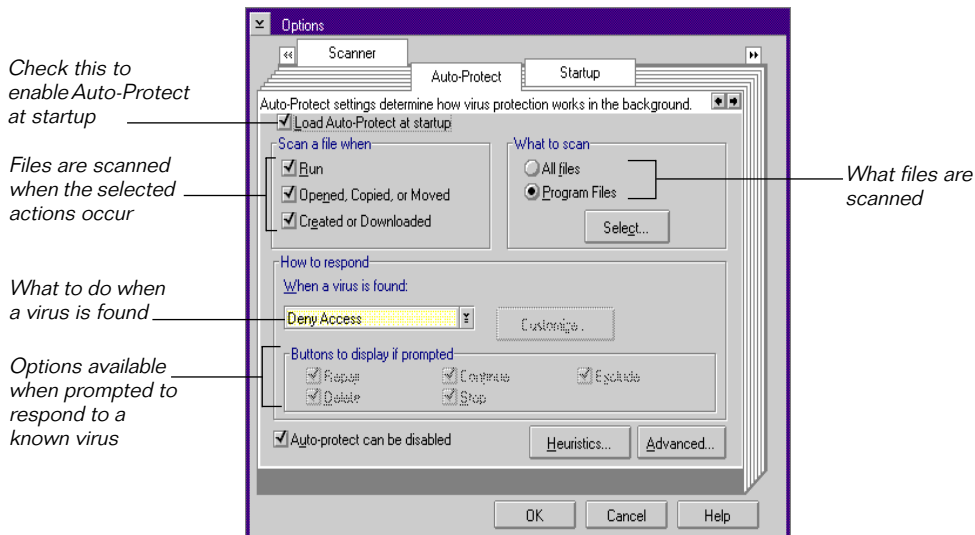
Note: Auto-Protect does not work in OS/2 native mode. This means that during any OS/2 Presentation Manager or command-line activities, such as copying, moving, or creating files, or downloading files from the Internet, floppy disks, or network drives, you are not automatically protected against viruses.

Monitoring the files you use

When enabled, Auto-Protect automatically checks for viruses whenever you open a file or run a program in a DOS or Win-OS/2 session. Monitoring files as they are used is the best protection to prevent viruses from infecting and spreading on your computer.

To monitor the files you use in Win-OS/2 and DOS sessions:

- 1 In the Options dialog box, click the Auto-Protect tab.



- 2 Specify in the Scan A File When group box when Norton AntiVirus should scan the files you use:

- **Run**
Scans a program file each time you run it in a DOS or Win-OS/2 session.
 - **Opened, Copied, or Moved**
Scans files whenever they are opened, copied or moved. For example, when you copy a file from one directory to another during a DOS or Win-OS/2 session, Norton AntiVirus scans the file you are copying.
 - **Created or Downloaded**
Scans files when they are created on your drive by an installation program, by compressing or uncompressing files, or by some other means. This includes files as they are downloaded from the Internet or Bulletin Board Systems (BBSs) within DOS and Win-OS/2 sessions.
- 3** Select an option in the What To Scan group box. For more information on which option to choose and on the program file extensions list, see “[Selecting which files to scan](#)” on page 51.
- **All Files**
Scans all files that you access in Win-OS/2 and DOS sessions. This includes files less likely to contain viruses.
 - **Program Files**
In Win-OS/2 and DOS sessions, scans files that are most likely to become infected. Only the files with extensions specified in the program file extensions list are scanned. To view or change the list of program file extensions, see “[Managing program file extensions](#)” on page 52.
- 4** Select an option in the When A Virus Is Found drop-down list box:
- **Deny Access**
Prevents you from copying, moving, or otherwise using a file when a known virus is detected. This is the default setting.
 - **Prompt**
Informs you when a known virus is found and lets you choose how to respond. Choose Prompt to have the most control over what happens to an infected file.
 - **Repair Automatically**
Repairs an infected file or boot record without notifying you. The outcome of the repair is recorded in the activity log.

- **Delete Automatically**
Deletes an infected file without notifying you. The name of the deleted file is recorded in the activity log.
Use caution when selecting this option. Files deleted by Norton AntiVirus cannot be recovered.
 - **Custom Virus Response**
Lets you access more options. For more information, see [“Customizing virus response”](#) on page 55.
- 5** If you selected Prompt in the previous step, specify in the Buttons To Display If Prompted group box which options you want Auto-Protect to make available when a known virus is found:
- **Repair**
Lets you repair the file or boot record.
 - **Delete**
Lets you delete the file. If the virus infects an item that cannot be deleted, such as a boot record, the button is dimmed.
 - **Continue**
Lets you continue accessing the file. If you click Continue when Norton AntiVirus alerts you, you may activate the virus.
 - **Stop**
Lets you stop accessing the file. The virus will not be activated, but the file is still infected.
 - **Exclude**
Lets you exclude the file from future checks for known viruses. Use caution when enabling this button; it reduces your protection against viruses.
- 6** Check Auto-Protect Can Be Disabled if you want to be able to disable Auto-Protect when you start up your computer. You can then use the options on the Startup Options dialog box to bypass loading Auto-Protect in a DOS or Win-OS/2 session.
- 7** If you selected Custom Response, you can specify further actions. For more information, see [“Customizing virus response”](#) on page 55.
- 8** Click OK.

Monitoring for unknown viruses

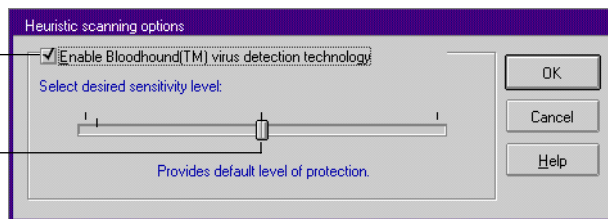
An unknown virus is one for which Norton AntiVirus does not have a definition. The Norton AntiVirus Bloodhound™ Virus Detection Technology monitors the files you access for unknown viruses. You can adjust the sensitivity level using the Heuristics button on the Auto-Protect Options dialog box. This feature is also available on the Scanner Options tab.

To scan for unknown viruses:

- 1 Click the Auto-Protect tab.
- 2 Click Heuristics.

Do you want Norton AntiVirus to check for unknown viruses?

Select the level of vigilance



- 3 In the Heuristic Scanning Actions dialog box, check Enable Bloodhound™ Virus Detection Technology to detect when your programs become infected by an unknown virus.
- 4 Drag the slider left or right to decrease or increase the sensitivity to virus-like activity.
- 5 Click OK.

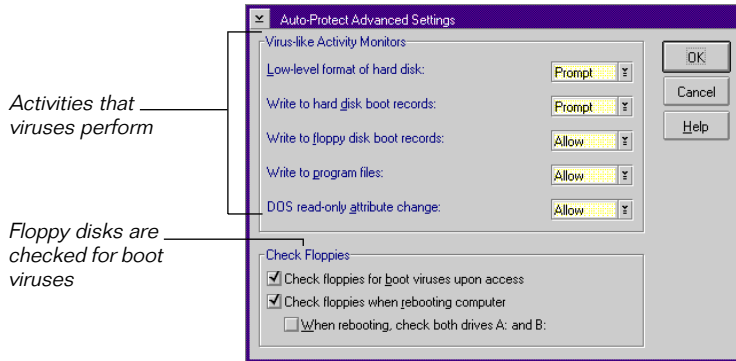
Monitoring for virus-like activities

A virus-like activity is an activity that many viruses perform when damaging your files or spreading through your system. Although some applications perform these actions for valid reasons, Norton AntiVirus can monitor for the activities on the chance that an unknown virus is performing one of them.

Note: These options apply to DOS and Win-OS/2 sessions only.

To monitor for virus-like activities:

- 1 In the Options dialog box, click the Auto-Protect tab.
- 2 Click Advanced.



- 3 In the Auto-Protect Advanced Settings dialog box, specify what Norton AntiVirus should do when it detects the virus-like activity. The virus-like activities include:

- **Low-Level Format Of Hard Disk**
All information on the disk is erased and cannot be recovered. This type of format is generally performed at the factory only. If this activity is detected, it almost certainly indicates an unknown virus at work.
- **Write To Hard Disk Boot Records**
Very few programs write to hard disk boot records. If this activity is detected, it could indicate an unknown virus at work.
- **Write To Floppy Disk Boot Records**
Only a few programs (such as the DOS Format command) write to floppy disk boot records. If this activity is detected, it could indicate an unknown virus at work.
- **DOS Read-Only Attribute Change**
Alerts when there is an attempt to change the DOS Read-Only attribute in a file.
- **Write To Program Files**
Some programs save configuration information within themselves. Although this activity often happens legitimately, it could indicate an unknown virus at work.

- 4 Select from the following responses for each of the options:
 - Prompt
Informs you when a program tries to perform the activity and lets you decide whether the activity should continue, stop, or be excluded for the program.
 - Allow
Allows the activity to continue every time without informing you. Selecting Allow offers you no protection against an unknown virus performing the activity.
 - Don't Allow
Prevents the activity from occurring every time it is detected.
- 5 Click OK.

Monitoring floppy disks

Because boot viruses are most likely to spread through floppy disks, it is important to check each floppy disk you use. Norton AntiVirus can monitor floppy disks when you work with them and when you leave them in your disk drives while pressing Ctrl+Alt+Del to reboot your computer. (These options offer no protection when you restart your computer using the power switch or the Reset button.)

Note: These options apply to DOS and Win-OS/2 sessions only.

To monitor floppy disks:

- 1 In the Auto-Protect tab, click Advanced to open the The Auto-Protect Advanced Settings dialog box.
- 2 In the Check Floppies group box, specify how you want Norton AntiVirus to check for boot viruses on floppy disks:
 - Check Floppies For Boot Viruses Upon Access
Checks for boot viruses on each floppy disk you access (such as, when you list the directory, copy a file, write to a file, or run a file).
 - Check Floppies When Rebooting Computer
Checks a floppy disk in drive A: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del.

- When Rebooting, Check Both Drives (A: and B:)

Also checks a floppy disk in drive B: for boot viruses when you restart your computer by pressing Ctrl+Alt+Del. Select this option if you have a system that can boot from a disk in the B: drive.

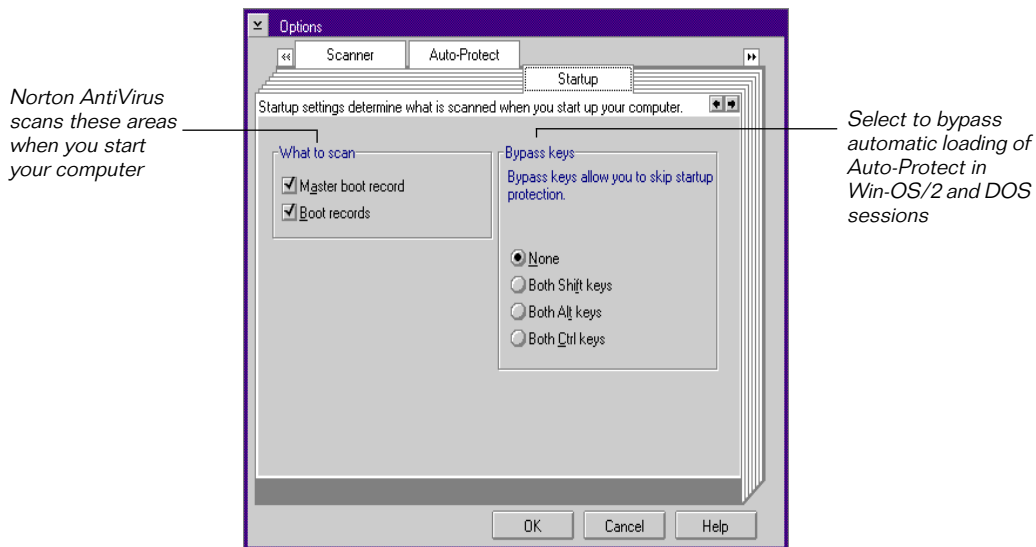
- 3 Click OK.

Customizing startup options

You can use the Startup options to define what Norton AntiVirus does when you start up your computer. These options include what to scan at startup, and how to control Auto-Protect loading during DOS and Win-OS/2 sessions.

To monitor during startup:

- 1 In the Options dialog box, click the Startup tab.



- 2 Specify in the What To Scan group box the areas that you want Norton AntiVirus to scan each time you start your computer:
 - Master Boot Record
Scans for boot viruses in the master boot record.
 - Boot Records
Scans for boot viruses in the boot records on your hard disk.

We recommend that you check all of these items.

- 3 Specify in the Bypass Keys group box the keystroke combination to prevent Auto-Protect from loading when you start a Win-OS/2 or DOS session from the Presentation Manager. When you hold down the selected keys, Auto-Protect will not load automatically. Your options are:

- None
- Both Shift Keys
- Both Alt Keys
- Both Ctrl Keys

Click None if you don't want a bypass key combination.

- 4 Click OK in the Auto-Protect Startup Settings dialog box.

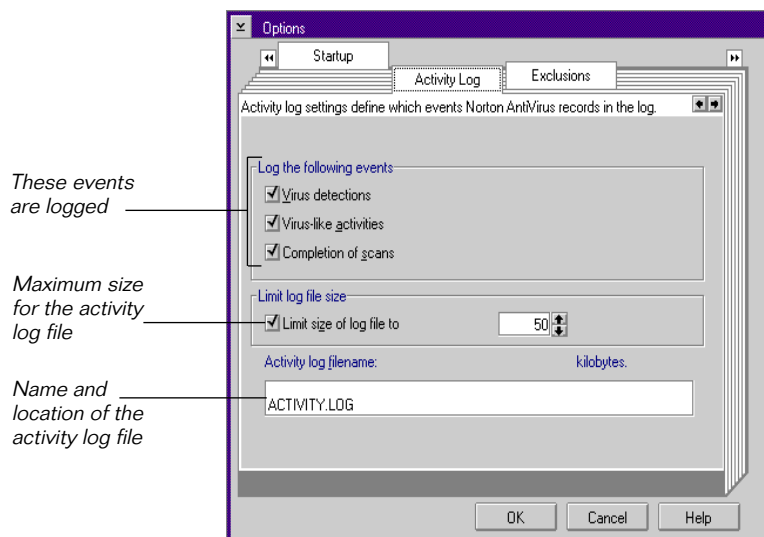
Customizing the activity log

You can specify the name and location for the activity log file, the types of events to record, and a maximum size for the file using the Activity Log category of options.

To customize the activity log:

- 1 In the Options dialog box, click the Activity Log tab.

The Activity Log settings appear.



- 2 In the Log Following Events group box, check each type of event that you want Norton AntiVirus to record:
 - **Virus Detections**
Records detections of known viruses.
 - **Virus-like Activities**
Records detections of virus-like activities, such as an attempt to format your hard disk.
 - **Completion of Scans**
Records the date and ending time of scans that you initiate.
- 3 If you want to limit the size of the activity log file, check Limit Size Of Log File To, then enter the desired size in the Kilobytes text box.

When the activity log reaches the specified size, each new entry added overwrites the oldest entry.
- 4 Enter the pathname for the activity log file in the Activity Log Filename text box.
- 5 Click OK.

Excluding files from scans

An exclusion is a condition or activity that would normally be detected during a scan that you have told Norton AntiVirus to ignore for a particular file. Norton AntiVirus uses the entries in the Exclusions List in all scans it performs.

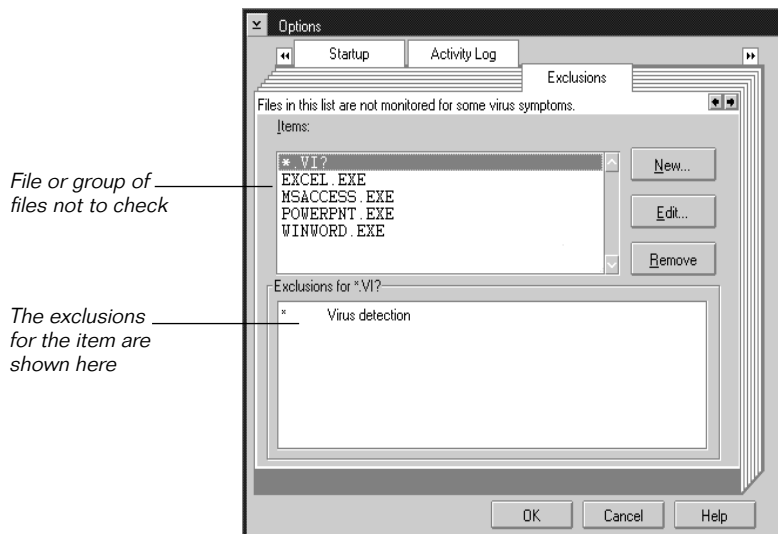
For example, since the Excel worksheet format, .XLS, is listed as a Program File in the Program File Extensions list because it is vulnerable to macro virus attacks, the Exclusions list includes EXCEL.EXE writing to program files so Norton AntiVirus doesn't interpret this as a virus attack.

Managing the exclusions list

The Exclusions List lets you manage the items that you have told Norton AntiVirus for OS/2 to ignore. You assign exclusions to items—drives, directories, groups of files, or single files. Each item can have more than one exclusion. If you move or rename a file, you automatically invalidate its exclusions.

To view the exclusions list:

- 1 Click the Exclusions tab.



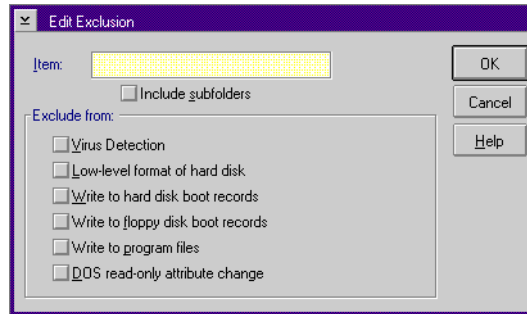
- 2 Select a file or group of files in the Items group box.
The activities excluded for the file or files are displayed in the Exclusions group box.
- 3 Click OK.

Adding an exclusion

In most cases, exclusions are added to the exclusions list when you click the Exclude button to resolve a problem that Norton AntiVirus has detected. You can also add exclusions to Norton AntiVirus manually.

To add exclusions manually:

- 1 In the Exclusions tab click New.



- 2 In the Edit Exclusion dialog box do one of the following:
 - Type the pathname for the file or group of files in the Item text box.
 - Click the Item browse button to choose a single file from a list, then click OK.
 If you enter a filename with no path, such as NAVOS2.EXE or JUNK.*, all files fitting that description are excluded.
 If you enter a full pathname, such as C:\SYMANTEC\NAVOS2.EXE or C:\JUNK.*, only files in that directory fitting that description are excluded.
 If you enter a directory, all files in the directory are excluded.
- 3 Check Include Subfolders if the item is a folder and you want its subfolders to be excluded as well.
- 4 Check the activities that you want Norton AntiVirus to ignore for the specified item.
 - Virus Detection
Exclude the item from checks for known viruses.
 - Low-Level Format Of Hard Disk
Exclude the item from checks for attempts to perform a low-level format of your hard disk, which obliterates all information on the disk.
 - Write To Hard Disk Boot Records
Exclude the item from checks for attempts to write to the boot records on your hard disk. This action is performed legitimately by very few programs.

- **Write To Floppy Disk Boot Records**
Exclude the item from checks for attempts to write to the boot record on a floppy disk. This action is performed legitimately by few programs.
- **Write To Program Files**
Exclude the item from checks for attempts to write to a program file. Some programs save configuration information within themselves rather than in a separate file.
- **DOS Read-Only Attribute Change**
Exclude the item from checks for attempts to change a file with a DOS read-only attribute so that it can be written to.

5 Click OK.

To edit or remove items in the exclusions list:

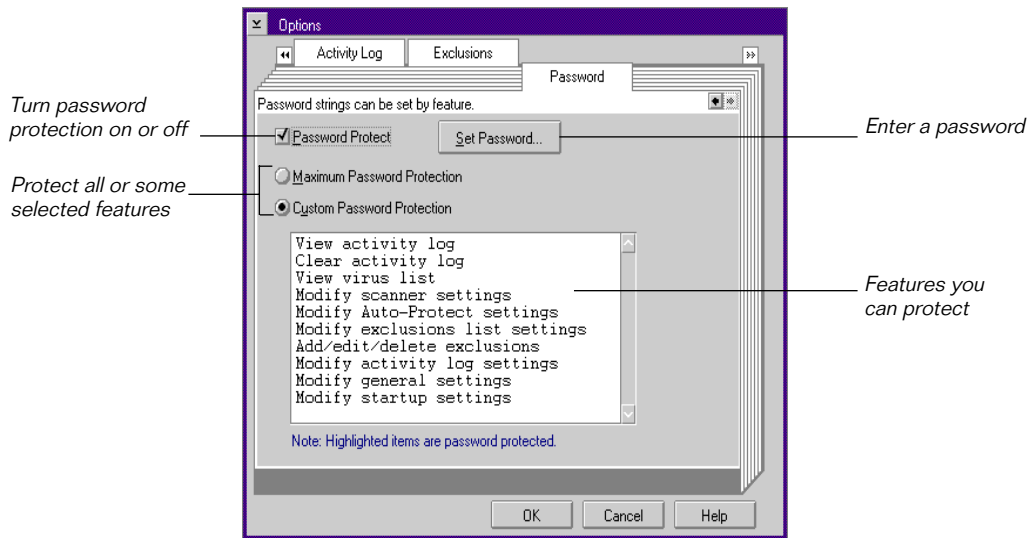
- 1** Select a file from the Items group box.
- 2** Do one of the following:
 - Click Edit to change the filenames or group of files designator. Change the appropriate settings in the Edit Exclusions dialog box.
 - Click Remove to delete the file from the list.
- 3** Click OK.

Password-protecting Norton AntiVirus

You can password-protect features of Norton AntiVirus to prevent others from making changes. For example, you may want to allow others to look at the virus list but not to delete virus definitions.

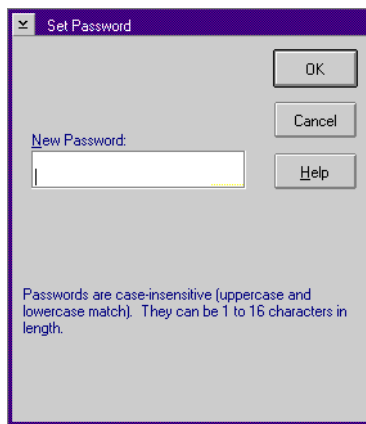
To password-protect features:

- 1 In the Options dialog box, click the Password tab.



- 2 Check Password Protect to turn on the password protection feature.
- 3 Select the level of password protection.
 - To protect all listed features, select Maximum Password Protection.
 - To protect specific features, select Custom Password Protection and then select the features you want protected.

- 4 Click Set Password.



- 5 Enter a password in the New Password text box and click OK. Enter it again in the Confirm New Password text box.

Passwords can be from 1 to 16 characters in length and are not case-sensitive (A is the same as a). As you type, Norton AntiVirus replaces the characters on the screen with asterisks (*) for security.

Note: Write down your password and store it in a secure place.

- 6 Click OK.

Password protection will activate the next time you start Norton AntiVirus. The password must be entered the first time you use a protected feature after you open Norton AntiVirus. Norton AntiVirus will also prompt for the password before allowing changes to these password protection options.

To change your password:

- 1 In the Options dialog box, click the Password tab.
- 2 Click Set Password.
- 3 Enter the old password in the Change Password dialog box, and click OK.
- 4 Enter the new password in the New Password text box, and click OK. Enter it again in the Confirm New Password text box.
- 5 Click OK in the Set Password dialog box.

The new password activates immediately.

Removing password protection

If you decide to no longer protect some or all of the features you have protected, you can remove password protection.

To remove password protection:

- 1 In the Options dialog box, click the Password tab.
- 2 Enter the existing password in the Verify Password dialog box.
- 3 Do one of the following:
 - If you want to remove password protection for some of the protected features, select Custom Password Protection and then deselect the features in the list box.
 - If you want to remove password protection completely, uncheck Password Protect.
- 4 Click OK.

Symantec Service and Support Solutions

Symantec is committed to excellent service worldwide. Our goal is to provide you with professional assistance in the use of our software and services, wherever you are located.

Technical Support and Customer Service solutions vary by country. If you have questions about the services described below, please refer to the section “Worldwide Service and Support” at the end of this chapter.

Registering your Symantec product

To register your Symantec product, please complete the registration card included with your package and drop the card in the mail. You can also register via modem during the installation process (if your software offers this feature) or via fax to (800) 800-1438 or (541) 984-8020.

LiveUpdate Subscription Policy

Retail customers: With the purchase of this product, you receive 12 free months of unlimited online use of LiveUpdate. Renewal subscriptions are available for \$3.95 per year.

After using this product for ten months, you will be prompted to subscribe when you begin a LiveUpdate session. Simply follow the onscreen instructions. After your one-year free subscription ends, you must renew your subscription before you can complete a LiveUpdate session.

To order, do one of the following:

- In the United States, call Customer Service at (800) 441-7234
- Outside the United States, contact your local Symantec office or representative
- Visit our website at: www.shop.symantec.com

Corporate Customers: Contact your Symantec representative for information about LiveUpdate subscription pricing.

Virus definitions update disk

If you don't have a modem to obtain virus definitions files using the Internet, CompuServe, America Online, or the Symantec BBS, you can order regular updates from Symantec to arrive by mail. This service requires a fee.

To order, do one of the following:

- In the United States, call (800) 441-7234.
- Outside the United States, contact your local Symantec office or representative.

Technical support

Symantec offers an array of technical support options designed for your individual needs to help you get the most out of your software investment.

World Wide Web

The Symantec World Wide Web site (<http://service.symantec.com>) is the doorway to a set of online technical support solutions where you will find the following services:

Interactive problem solver

Symantec's online interactive problem solver (known as the Support Genie) helps you solve problems and answer questions about many Symantec products.

Product knowledgebases

Product knowledgebases enable you to search thousands of documents used by Symantec Support Technicians to answer customer questions.

FAQs

Frequently Asked Questions documents, also known as FAQs, list commonly asked questions and clear answers for specific products.

Discussion groups

Discussion groups provide a forum where you can ask questions and receive answers from Symantec online support technicians.

FTP

Point your web browser to <http://service.symantec.com> to search for and download technical notes and software updates. You can also click the LiveUpdate button in programs enabled with this feature to automatically download and install software updates and virus definitions.

Other Symantec support options include the following:

America Online	Type Keyword: SYMANTEC to access the Symantec forum.
CompuServe	Type GO SYMANTEC to access the Symantec forum.
Symantec BBS	Set your modem to 8 data bits, 1 stop bit, no parity and dial (541) 484-6669.
Automated fax retrieval system	<p>To receive general product information, fact sheets and product upgrade order forms directly to your fax machine, please call our Customer Service fax retrieval system at (800) 554-4403 or (541) 984-2490.</p> <p>For technical application notes, please call our Technical Support fax retrieval system at (541) 984-2490 and select option 2.</p>
StandardCare Support	<p>If you can't access the Internet, take advantage of your 90 days of free telephone technical support (from the date of your first call) at no charge to all registered users of Symantec software.</p> <p>Please see the back of this manual for the support telephone number for your product.</p>
PriorityCare and PlatinumCare Support	Expanded telephone support services are available to all registered customers. For complete information, please call our automated fax retrieval service, located in the United States, at (800) 554-4403 or (541) 984-2490, and request document 070, or visit www.symantec.com/techsupp/phone/index.html

Chat Now!

Chat Now! For selected products this service provides customers with the ability to discuss technical issues with a Support Analyst in “realtime” over the Internet, using text, files, and HTML for a fee.

Support for old and discontinued versions

When a new version of this software is released, registered users will receive upgrade information in the mail. Telephone support will be provided for the previous version for six months after the release of the new version. Technical information may still be available through online support.

When Symantec announces that a product will no longer be marketed or sold, telephone support will be discontinued 60 days later. Support will only be available for discontinued products through online services. See the section “Technical support” for online service options.

Customer Service

Symantec’s Customer Service department can assist you with non-technical questions. Call Customer Service to:

- Order an upgrade.
- Subscribe to the Symantec Support Solution of your choice.
- Fulfill your request for product literature or demonstration disks.
- Find out about dealers and consultants in your area.
- Replace missing or defective CDs, disks, manuals, etc.
- Update your product registration with address or name changes.

You can also visit Customer Service online at www.symantec.com/custserv for the latest Customer Service FAQs, to find out the status of your order or return, or to post a query to a Customer Service discussion group.

Worldwide Service and Support

Symantec provides Technical Support and Customer Service worldwide. Services vary by country and include International Partners who represent Symantec in regions without a Symantec office. For general information, please contact the Symantec Service and Support Office for your region.

Service and Support offices

NORTH AMERICA

Symantec Corporation	(800) 441-7234 (USA & Canada)
175 W. Broadway	(541) 334-6054 (all other locations)
Eugene, OR 97401	Fax: (541) 984-8020
Automated Fax Retrieval	(800) 554-4403
	(541) 984-2490

BRAZIL

Symantec Brazil	+55 (11) 5561 0284
Av. Juruce, 302 - cj 11	Fax: +55 (11) 5530 8869
São Paulo - SP	
04080 011	
Brazil	

EUROPE

Symantec Ltd.	+31 (71) 408 3111
Schipholweg 103	Fax: +31 (71) 408 3150
2316 XC Leiden	
The Netherlands	
Automated Fax Retrieval	+31 (71) 408 3782

ASIA/PACIFIC RIM

Symantec Australia Pty. Ltd.	+61 (2) 9850 1000
408 Victoria Road	Fax: +61 (2) 9850 1001
Gladesville, NSW 2111	
Australia	
Automated Fax Retrieval	+61 (2) 9817 4550

Most International Partners provide Customer Service and Technical Support for Symantec products in your local language. For more information on other Symantec and International Partner locations, please call our Technical Support automated fax retrieval service, in the United States at +1 (541) 984-2490, choose Option 2, and request document 1400.

Every effort has been made to ensure the accuracy of this information. However, the information contained herein is subject to change without notice. Symantec Corporation reserves the right for such change without prior notice.

I N D E X

A

- activity log
 - customizing, 64–65
- alerts
 - guide to actions, 40
 - responding to virus found, 37–40
 - types, 40
- applications
 - virus-like activities, 39–40
- Auto-Protect
 - bypassing at startup, 64
 - customizing, 57–63
 - file scan options, 57
 - floppy disk options, 62
 - startup options, 63
 - virus-like activity options, 60
 - enabling for Win-OS/2 sessions, 26, 42
 - protection in OS/2, 16
 - scanning at startup, 63

B

- Bloodhound technology, 56, 60
- boot records
 - checking for viruses, 49
 - scanning at startup, 63
 - unable to repair in OS/2, 43
- bulletin board systems
 - scanning downloaded files, 58

C

- categories. *See* options
- CD-ROM
 - installing Norton AntiVirus for OS/2, 11
- checking for viruses
 - at startup, 63
 - in boot records, 49

- checking for viruses (*continued*)
 - in compressed files, 49
 - in files, 51
 - on floppy disks, 62
- compressed files
 - repairing, 42–43
 - scanning, 17, 49
- computer system
 - virus behavior, 15
- Continue alert action button, 40
- customizing
 - activity log, 64–65
 - Auto-Protect, 57–63
 - Norton AntiVirus for OS/2, 47–71
 - password protection, 69
 - program file extensions, 51
 - response when virus is found, 50, 59
 - scanning, 49–53

D

- decompressing files. *See* compressed files
- Delete alert action button, 40
- deleting
 - files automatically, 50, 59
 - infected files, 40, 41
 - program file extensions, 53
- directories
 - excluding from scans, 67
 - scanning for viruses, 22
 - selecting installation, 12
- disabling/enabling Auto-Protect, 26
 - when decompressing files, 42
- disk space requirements
 - for installing
 - Norton AntiVirus for OS/2, 10
- DOS Emergency Boot Disk
 - restarting with, 44
 - restoring system files after use, 45

- downloads
 - automatic scanning for viruses, 17
 - virus definitions via LiveUpdate, 28
- drives
 - scanning network, 21
- drives, scanning for viruses, 20

E

- emergency
 - action if infected, 10
- Emergency Boot Disk. *See* DOS Emergency Boot Disk
- enabling/disabling Auto-Protect, 26
 - in Win-OS/2 and DOS sessions, 42
- Exclude alert action button, 40
- excluding files from
 - virus detection, 67
 - virus-like activity detection, 67–68
- exclusions list, 65
 - adding entries, 66
- exiting Norton AntiVirus, 19
- extensions. *See* program file extensions

F

- file extensions. *See* program file extensions
- files
 - checking for viruses, 50, 58
 - excluding from scans, 66
 - monitoring for viruses, 57
 - reinfected after virus removal, 42
 - scanning for viruses, 22
 - stopping access, 58
- floppy disks
 - monitoring for viruses, 62
 - scanning for viruses, 19
 - unable to repair boot record, 43
- folders
 - scanning for viruses, 22

H

- hard disk
 - checking at startup, 63
 - monitoring for viruses, 57
- Heuristics setting, 56, 60

I

- infected files
 - action if reinfected, 42
 - deleting automatically, 50
 - unable to repair, 41
- installing
 - Norton AntiVirus for OS/2, 9
 - configuration options, 12
 - procedure, 10–11
 - system requirements, 10
 - questions during install, 12
 - what to do next, 13
- Internet
 - virus protection during access, 17

K

- known viruses
 - customizing checks for, 57
 - customizing scan options, 49

L

- LiveUpdate
 - obtaining virus updates via, 28
 - scheduling regular events, 25
- logging
 - Norton AntiVirus activities, 65

M

- master boot record
 - checking at startup, 63
 - checking for viruses, 49
 - replacing in OS/2, 43

modifying
 password, 70
 program file extensions list, 52
monitoring for viruses
 at startup, 63
 on floppy disks, 62
 virus-like activities, 60

N

network
 drives, scanning, 21
Norton AntiVirus for OS/2
 Auto-Protect, 26
 customizing, 26
 DOS Emergency Boot Disk, 44
 exiting, 19
 features, 17
 icons, 13
 installing, 9
 configuration options, 12
 procedure, 10–11
 system requirements, 10
 starting, 18

O

online help, Norton AntiVirus for OS/2, 19
opening Norton AntiVirus for OS/2, 18
options, 48
 activity log, 64–65
 automatic protection, 57
 exclusions list, 66
 password protection, 69
 scanning, 49
OS/2, 16
 DOS sessions and Auto-Protect, 16
 Start-up floppy disks, 45
 Win-OS/2 sessions and Auto-Protect, 16

P

password protection
 changing password, 70
 removing password, 71
 setting password, 69
PKUNZIP, 42
Problems Found dialog box, 38
program file extensions, 51, 52, 53
 adding, 52
 resetting default list, 53

R

removing viruses
 deleting infected files, 41
 repairing files, 39
Repair alert action button, 40
repairing
 compressed infected files, 42, 43
 infected files, 40
 automatically, 58
 unsuccessfully, 41
 infected files unsuccessfully, 43
requirements
 for installing, 10
restoring
 program file extensions list, 53

S

scanner options, 49
scanning
 drives, 20
 files or folders for viruses, 22
 network drives, 20
scans
 customizing, 49–53
 excluding files, 65
 scheduling, 23
Scheduler. *See* scheduling
scheduling
 LiveUpdate events, 25
 virus scans, 23

- software
 - avoiding infected, 18
 - disabling virus protection when installing, 26
- starting
 - Norton AntiVirus for OS/2, 18
- startup files, OS/2, 12
- Stop alert action button, 40
- stopping file access, 58
- system files, 45
 - damaged by virus in OS/2, 43
- system requirements
 - for installing, 10

U

- uncompressing files for repair, 42
- uninstalling Norton AntiVirus for OS/2, 14
- unknown viruses
 - scanning for, 56, 60
- updating
 - virus protection, 17, 28
- utility disks
 - for emergency restart in OS/2, 45

V

- virus alerts, 37–40
- Virus Found alert, 39
- virus protection
 - by Norton AntiVirus for OS/2, 17
 - disabling/enabling, 26
 - keeping current, 28–30
 - updating frequently, 17
 - user responsibilities, 17
- viruses
 - avoiding, 18
 - behavior, 15
 - in OS/2 environment, 16
 - release of new, 28
 - removing before installing, 10
- virus-like activities
 - alerts, 39, 40
 - monitoring for, 60

W

- Windows
 - Win-OS/2 sessions and Auto-Protect, 16
- WinZip, 42